EFEMERAL GRAF VISUALISASI (EGV) BAGI PENGESANAN MUSUH SIBER MELALUI PELAN MITRE ATT&CK DAN PEMBELAJARAN MENDALAM

AHMAD ASYRAF BIN MUSTAFAR

ASSOC. PROF. DR. SITI NORUL HUDA SHEIKH ABDULLAH

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

ABSTRAK

Dalam menghadapi ancaman serangan siber yang semakin meningkat, terdapat keperluan yang mendesak bagi strategi pengesanan dan pengenalpastian ancaman yang inovatif. Kajian ini menggupas tentang pengkatogerian ancaman siber pengesanan anomali dengan cara menggabungkan kerangka kerja MITRE ATT&CK dan model pembelajaran mendalam. Kerangka kerja Att&CK yang terkenal dan diakui secara global menawarkan taksonomi yang sistematik terhadap maklumat ancaman siber (CTI), dimana ianya menekankan analisis ancaman secara mendalam. Melalui penggabungan pembelajaran mendalam dengan kerangka kerja ini, kajian ini memudahkan pengembangan perspektif terhadap corak taktik, teknik dan prosedur (TTP) yang berbilang, sebagaimana yang telah digariskan di dalam kerangka tersebut. Model pembelajaran mendalam, yang menerusi rangkaian neural menunjukkan potensi kemampuan yang tinggi dari segi pembelajaran dinamik, dimana ianya dapat mengemas kini keupayaan pengesanan ancaman mengikut taksonomi ATT&CK yang berkembang secara berterusan, secara tidak langsung memastikan pengekalan relevansi maklumat dalam persekitaran ancaman siber yang kerap berubah. Selanjutnya kajian ini juga memperkenalkan kelebihan dari segi penggabungan arkitektur ancaman, khususnya dalam Ekspresi Informasi Ancaman Terstruktur / Pertukaran Automatik Dipercayai oleh Informasi Petunjuk (STIX/TAXII), dengan paradigma pembelajaran mendalam untuk menganalisis data skala besar, sejajar dengan metodologi DevSecOps, dimana ianya menyajikan strategi ke hadapan untuk pendekatan langkah keselamatan siber yang lebih adaptif. Penekanan yang diberikan dalam kajian ini berpusat dengan pengenalan bagi efemeral graf visualisasi (EGV), dimana ianya menerapkan penggunaan model peluruhan bagi menentukan relevansi maklumat, dengan kemampuan untuk menetapkan semula ingatan berdasarkan insiden atau peristiwa tertentu. Hal ini merupakan inovasi jika dibandingkan dengan kaedah konvensional yang sedia ada. Kesan daripada inovasi ini, analisa keselamatan (SA) dapat menjimatkan masa pada proses korelasi insiden, justeru meningkatkan prestasi perkhidmatan dan waktu maklumbalas. Bagi set data untuk kajian ini pula, ianya diperoleh secara masa nyata dari platform awanan. Data yang diperoleh akan melalui proses sanitasi data yang melibatkan normalisasi, Regex, perwakilan dan strim maklumat ancaman menerusi saluran ETL, sebelum aturan petua dilakukan pada SIEM. Attribut ditentukan dahulu untuk proses pengenalpastian semasa pemetaan saluran dijalankan

bagi memudah proses orkestrasi bagi input seterusnya. Sementara itu, dasar bagi (IDS) juga membantu pakar subjek (SME) dalam membentuk model pembelajaran mendalam (DLM) pada peringkat awal. Dengan latihan yang berterusan. Penemuan awal menunjukkan bahawa EGV menawarkan kaedah yang lebih intuitif dan cepat dalam mentafsirkan landskap serangan ancaman yang rumit berbanding kaedah tradisional yang mana menerusi navigasi layar dan saringan lapisan data. EGV memaparkan entiti data sebagai "nod" dan hubungan antaranya sebagai "edge" dalam mencipta graf yang komprehensif. Kajian ini menandakan pendekatan transformasi dalam manafsirkan dan memaklumbalas kepada CTI

PENGENALAN

Bidang keselamatan siber adalah sebuah sektor teknologi yang bukan lagi menjadi sisi tersembunyi dalam kehidupan harian kita yang rata-rata kini terhubung secara digital, ianya telah terbentuk dan bertumbuh dengan pesat dalam menduduki carta kepentingan teratas di dalam hierarki transformasi teknologi digital. Hal ini dapat dilihat menerusi peningkatan permintaan yang tinggi dalam kalangan masyarakat dan juga industri yang rata-rata telah bergerak mengikut arus pemodenan digital berikutan kesan daripada wabak covid-19 yang telah melumpuhkan sebahagian besar ekonomi dari segenap pelusuk dunia pada lingkungan tahun 2018-2021. Ditambah pula dengan kerumitan ancaman siber yang kian berevolusi saban hari, Pendekatan keselamatan siber secara tradisional tidak lagi mampu memberi kesan yang efektif dan optimal akibat terus dicabar oleh strategi-strategi canggih yang dikendalikan oleh musuh siber (Lakshmi Narayanan Kaliyaperumal 2021). Oleh itu, terdapat trend pertambahan permintaan yang ketara terhadap perkembangan strategi pengesanan dan pengkelasan ancaman, dimana strategi tersebut mestilah mempunyai keupayaan untuk turut berkembang seangkatan dengan peredaran arus waktu perdana dan juga landskap digital.

Pergantungan masyarakat terhadap sistem dan rangkaian digital telah menjadikan keselamatan siber sebagai salah satu komponen terpenting bagi memastikan infrastruktur yang kukuh dalam menghadapi ancaman siber (Kuner 2017). Walaubagaimanapun, untuk mengenal pasti ancaman serta mengklasifikasikannya bukanlah perkara yang mudah, ianya antara cabaran terbesar dalam era digital ini. Hal ini kerana sebelum memahami atau memerangi suatu perkara, langkah serta kaedah yang paling efektif perlulah ditekankan terlebih dahulu sebagai garis panduan bagi mendalami corak pemikiran serta kelakuan musuh. Beberapa model pengenalpastian yang efektif telah dikaji dan dibangunkan bagi menyelasaikan permasalahan ini. Antaranya, terdiri daripada "Diamond Model", "Cyber Kill- Chain Model" dan juga "Mitre Att&ck Model" (N. Naik 2022). Berikut merupakan tiga model yang menduduki carta teratas dan seringkali digunakan sebagai garis panduan bagi penyiasatan ancaman siber menerusi jalur peredaran zaman. Rangka kerja Mitre Att&ck merupakan satu insiatif yang dilancarkan oleh "MITRE Corporation" pada tahun 2013 bagi menyediakan sokongan teknikal. Model ini dibangunkan sebagai sumber rujukan untuk mengenalpasti dan mendokumentasikan taktik, teknik dan prosedur (TTPs) yang digunakan oleh penggodam dalam persekitaran jaringan korporat dan membantu memperkembangkan strategi pertahanan siber yang lebih efektif (Anna Georgiadou 2021).

Dari lensa Maklumat Ancaman Siber (CTI) pula, “Mitre Att&ck Model” merupakan suatu entiti berharga yang mampu menganilisa pengetahuan atau indikator yang diperoleh dalam menghubungkan suatu kaitan jenayah kepada bebenang seterusnya (P. R. Vishnu 2021). Ia juga dapat membantu dalam proses pengenalpastian ancaman, perkembangan strategi, peningkatan kesedaran, kolaborasi komuniti dan juga penilaian risiko. Disebabkan faktor-faktor tersebut, Model ini dipilih khusus kerana mempunyai struktur pemetaan ancaman yang menyeluruh dibandingkan dengan model lainnya. Secara amnya, model Mitre juga merupakan sebuah standard yang dipraktikkan dan diperakui oleh industri-industri keselamatan siber dari segenap penjuru dunia. Walhal pada dasarnya, CTI hanyalah sebuah platform yang merujuk kepada informasi yang dikumpulkan bagi memahami sikap atau jenis ancaman siber yang mungkin dihadapi oleh sesebuah organisasi. Namun, dengan adanya rangka “Mitre Att&ck Model”, organisasi dapan melihat gambaran yang lebih mendalam tentang ancaman siber serta memahami bagaimana cara musuh bekerja dan berfikir. Meskipun dengan pengenalan model ini dapat sedikit sebanyak membantu para analisa dari sudut pengkelasan ancaman, hakikatnya cara ini masih lagi digelarkan sebagai pendekatan yang manual kerana ianya masih memerlukan campur tangan manusia dalam proses korelasi insiden dan alur kerja pemetaan ancaman.

Berikutan dari hal di atas, pembelajaran mendalam merupakan salah satu kaedah yang boleh ditekankan dalam konteks pengkelasan ancaman secara automatik. Ia merupakan salah satu cabang dalam kecerdasan buatan yang menggunakan rangkaian neural tiruan untuk belajar membuat keputusan berdasarkan data. Rangkaian ini membolehkannya untuk memproses maklumat dengan lebih kompleks berbanding teknik kecerdasan buatan tradisional. Dengan pembelajaran mendalam, sistem boleh dilatih untuk mengenali pola-pola tertentu dalam mengenalpasti tabiat, sikap atau corak serangan dengan lebih mendalam dan cepat. Hal ini memudahkan serta menjimatkan masa para analisa daripada harus merungkai setiap jenis serangan dan kolerasi insiden secara manual. Kajian ini dijalankan untuk meneroka bagaimana integrasi antara rangka kerja “Mitre Att&ck Model”, Maklumat Ancaman Siber dengan pembelajaran mendalam boleh meningkatkan pemahaman dan penanganan organisasi terhadap ancaman siber. Hasilan dapatan membuahkan suatu penemuan idea baru bagi penambahbaikan metodologi penyiasatan sedia ada: penemuan metodologi ini digelar sebagai “Ephemeral Graph-Based Visualization” (EGV). Metodologi ini terbukti memberi perspektif dan nafas baru terhadap dunia sumber maklumat dimana semua data diperhalusi dan dihubungkan melalui jaringan nod dan menggunakan sepenuhnya idea data efemeral untuk mengeliminasi masa yang diambil untuk ketersediaan maklumat melalui proses “Data Query” (P. R. Vishnu 2021).

METODOLOGI KAJIAN

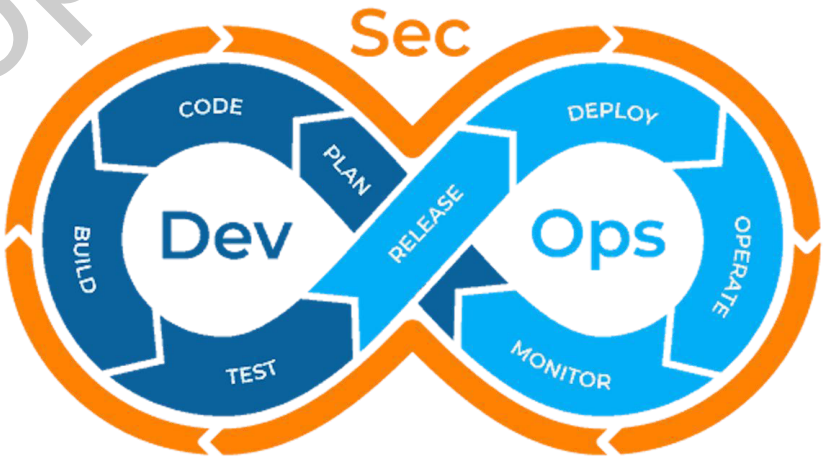
Kitaran hayat pembangunan perisian (SDLC) adalah proses yang standard digunakan di dalam mana-mana industri yang melibatkan pembangunan dan penyelidikan bagi tujuan merancang, mengembangkan, menguji serta membangunkan sesebuah perisian. Di dalam konteks kajian ini, metodologi “DevSecOps” dan juga “Agile” merupakan dua pendekatan di dalam SDLC yang digunapakai bagi memperoleh hasil kajian. Dengan pendekatan kedua

metodologi yang unik ini, kitaran hayat pembangunan perisian dapat diperkayakan dan juga dimodenkan sejajar dengan kualiti landskap digital di dalam arus perdana.

Pemilihan metodologi DevSecOps beserta Agile di dalam kajian ini membawa alasan yang kukuh, terutamanya di dalam lingkungan pembangunan sistem saling kendali dengan integrasi perkhidmatan terurus yang mengutamakan keselamatan dari prospek segala ancaman fizikal mahupun natural tanpa perlu mengorbankan kecekapan dan kelancaran dalam penghantaran hasil. DevSecOps menekankan integrasi keselamatan dalam setiap aspek pembangunan sistem bagi memastikan ianya diberikan perhatian dari awal fasa penubuhan. Ianya sejajar dengan prinsip-prinsip Agile yang menggalakkan penyesuaian dan penambahbaikan secara berterusan.

Integrasi ini tidak hanya memperkuat aspek keselamatan dalam pembangunan malah juga menjamin penerapan praktis yang standard daripada industri di dalam proses pembentukan oreksetrasi alur kerja yang mungkin melibatkan teknologi seperti CI/CD mahupun IAC. Penglibatan teknologi-teknologi sebegini membolehkan pengkajian semula serta penambah baikan dari aspek keselamatan dilakukan secara beransur mahupun berterusan tanpa perlu menganggu alur kerja yang telah diautomasikan. Selain itu, kedua-dua metologi ini juga turut melengkapi budaya kerja yang mempromosikan kolaborasi dan komunikasi, sekaligus mengurangkan risiko kesalahan pada tahap-tahap akhir di dalam proses pembangunan yang seringkali memerlukan kos yang mahal dan rumit untuk diperbaiki.

Kesimpulannya, pemilihan metodologi ini secara bersamaan mencipta keseimbangan antara keperluan bagi penghantaran yang lebih peka dan responsif terhadap permintaan pihak berkepentingan serta pematuhan yang ketat di dalam piawaian keselamatan bagi memastikan keselamatan sistem yang komprehensif dan mendalam. Kedua-dua metodologi ini bukan sahaja melengkapi antara satu sama lain malah juga membentuk satu pendekatan yang holistik untuk pembangunan sistem di dalam dunia yang sentiasa berubah dan penuh dengan ancaman digital ini.



Fasa Perancangan

Fasa perancangan adalah fasa dimana sesebuah tujuan dan keperluan sistem ditentukan bagi kajian EGV in, fasa ini melibatkan perancangan "sprint" dan penetapan "backlog" untuk membolehkan maklumbalas dan pendapat diutarakan semasa sesi perjumpaan, maklumbalas tersebut diambil kira untuk penambahbaikan selama proses pembangunan sistem ini berjalan. Seawal fasa ini juga, penetapan keamanan dalam arkitektur diberikan perhatian untuk pembangunan yang selari dengan piawaian keselamatan.

Fasa Reka Bentuk

Pada fasa reka bentuk pula, pembangunan bagi pangkalan data serta algoritma struktur bagi sistem EGV diambil kira melalui modul yang telah diperincikan di dalam spesifikasi keperluan fungsian dan juga bukan fungsian, manakala reka bentuk antaramuka pula dibina berdasarkan maklumbalas daripada sasaran pengguna, di mana ini telah dinyatakan di dalam sesi wawancara. Kaedah ini memberi pendekatan yang bersifat iteratif dan fleksibel jika ada perubahan yang perlu dilakukan tanpa perlu menunggu sesebuah komponen untuk selesai dibangunkan sepenuhnya.

Fasa Pembangunan

Seterusnya adalah fasa pembangunan. Di mana sejurus selesainya fasa reka bentuk serta arkitektur EGV, fasa ini melibatkan penulisan kod dan implementasi fungsi-fungsi sistem. Kaedah yang digunakan untuk pembangunan sistem EGV ini adalah dengan cara membahagi tugasan modul utama kepada potongan yang kecil, dan bagi setiap komponen kecil fungsi utama pula, ianya hanya mengandungi kod berkaitan sahaja. Praktis ini menekankan konsep "DRY" di dalam penulisan kod pembangunan EGV dimana penekanan yang diberikan kepada penggunaan semula fungsi adalah dititikberatkan. Pada fasa ini, pembangunan EGV masih lagi berada pada "local environment".

Fasa Pengujian

Fasa pengujian ini pula dilakukan selepas selesainya fasa pembangunan, ianya untuk memastikan fungsi, kualiti dan keamanan kod tercapai. Proses ini akan dilakukan pada setiap kali komponen atau modul baru bagi EGV diperkenalkan kedalam induk repositori, perubahan dalam repositori hanya akan dibenarkan jika semua fungsi pada modul atau komponen tersebut berjaya melepasi kesemua ujian yang dijalankan pada fasa ini.

Fasa Semakan

Dalam fasa semakan pula, peninjauan komponen bagi fungsi-fungsi utama sistem akan dilakukan untuk merujuk kembali sama ada fungsi yang dibangunkan memenuhi syarat bagi tujuan asal dalam perancangan sistem, dalam pembangunan EGV, proses ini dilakukan melalui semakan berkala “sprint”, dimana maklumbalas bagi setiap fungsi akan dicatat dan

penambahbaikan fungsi akan dilakukan sebelum lanjut ke fungsi lain. Kod pembangunan juga akan dinilai tahap keamanannya sama ada ianya ditulis mengikut piawaian yang standard ataupun sebaliknya.

Fasa Pelaksanaan

Fasa ini memastikan bahawa kod yang telah diuji dan disemak akan di aplikasikan ke dalam lingkungan produksi, proses ke produksi mengandungi tiga langkah, dimana pengujian kod EGV yang berjaya akan membawa pembangunan yang dibangunkan pada "local environment" kepada platform awanan. Pada platform produksi, sebuah gerbang API akan dibangunkan bagi pengelolaan servis baharu. Bagi setiap modul yang berkenaan dengan port servis baharu, ianya perlu dibenarkan terlebih dahulu di dalam polisi rangkaian platform awanan, kemudiannya "route mapping" perlu di definisikan pada "gateway" bagi memastikan trafik yang diterima dari internet menghala kepada destinasi yang betul.

Fasa Operasi

Bagi fasa ini pula, ianya melibatkan lebih kearah metodologi DevSecOps iaitu pengurusan sistem secara aktif. Peninjauan operasi adalah pendekatan yang penting untuk dilakukan bagi memastikan alur kerja operasi mampu memberikan kualiti yang terbaik dengan tenaga kerja yang minima, fasa ini sering mengadaptasi pelbagai jenis integrasi teknologi bagi memudahkan operasi untuk bertindakbalas dengan lebih pantas terhadap respon mahupun eskalasi insiden dari EGV. Dengan integrasi pelbagai teknologi di dalam alur kerja, sistem mampu diprogramkan untuk melakukan perkara tanpa memerlukan campur tangan luar.

Fasa Pemantauan

Bagi sifat organisasi seperti AceTeam, fasa pemantauan adalah pendekatan yang penting untuk dilakukan bagi menguji sama ada keberkesanan solusi semasa mampu menangani perubahan dalam taktik serangan musuh. Oleh yang demikian, pemantauan yang berterusan adalah penting bagi menambahbaik “backend” EGV dari algoritma ke model pembelajaran serta pengecaman taktik dan teknik terkini.

KEPUTUSAN DAN PERBINCANGAN

Dalam proses pembangunan solusi EGV ini, terdapat beberapa jenis rangka kerja yang telah dipilih khusus bagi pembentukan solusi ini, antaranya adalah penggunaan rangka kerja MITRE, rangka kerja orkestrasi, Tailwind, React, NextJS, Swagger bagi komponen utama bahagian depan. Manakala Django, Docker, PostgreSQL, Kafka, PyTorch, Ossec sebagai komponen utama bahagian belakang. Bahasa pengaturcaraan utama yang digunakan pula adalah Python dan Javascript. Solusi ini dibangunkan pada persekitaran virtual yang dikendalikan oleh aturan CI/CD bagi memastikan kualiti perisian yang dibina patuh kepada piawaian yang digunapakai oleh industri keselamatan siber. Sebuah persekitaran telah dibina

bagi melengkapi segala kriteria yang telah dikemukakan. Berikut merupakan antara komponen yang telibat bagi memenuhi keperluan pada persekitaran solusi:

Studio Visual Kod (IDE)

Sebagai permulaannya, studio visual kod (IDE) telah dipilih sebagai platform bagi pembangunan keseluruhan usulan dan rangka projek bagi solusi yang dicadangkan. Persekitaran pembangunan bersepadu (IDE) ini merupakan perisian yang digunakan bagi menawarkan pelbagai jenis fungsi dan perkhidmatan yang memudahkan pengaturcara dalam mengembangkan, menguji, dan menyelenggara aplikasi perisian. Ianya turut juga menyediakan pelbagai rangka kod untuk mempercepatkan lagi proses pembangunan sistem, di samping penyokongan fungsi penyorotan sintaks dan penyelesaian kod automatik, ia juga mampu membuat kompilasi dari pelbagai jenis bahasa kod, kolaborasi bersama Git dan menyelesaikan ralat sintaks. Justeru itu, perisian ini digunakan bagi mempercepat dan melancarkan proses pembangunan kod perisian.

Persekitaran Maya

Seterusnya, bagi memperhalusi lagi alur pembangunan perisian, persekitaran maya telah digunapakai bagi mengaplikasikan ruang privasi untuk setiap versi baru. Ianya bertujuan untuk mengasingkan setiap komponen pergantungan "dependency" kepada ruang versi mereka tersendiri supaya ianya tidak menganggu senarai komponen kebergantungan induk. Oleh itu, setiap persekitaran hanya mengandungi komponen yang diperlukan sahaja, dan secara tidak langsung dapat mengurangkan perimeter serangan. Selain itu, pengguna juga dapat memelihara keserasian antara pustaka- pustaka yang digunakan dan versi kod yang disokong oleh projek tersebut dan berkongsi konfigurasi perisian pada peranti lain seperti persekitaran dan kebergantungan pustaka asalnya, ini sekaligus memudahkan kolaborasi antara ahli projek yang bekerja dari pelbagai komputer atau persekitaran. Setiap individu boleh membuat persekitaran maya mereka sendiri dengan keperluan projek yang sama, menjadikan pengembangan dan pengujian projek lebih selaras. Amalan ini amat dititikberatkan di dalam produksi industri yang mempraktiskan "DevSecOps"

Kontena

"Docker" merupakan platform yang membolehkan pembangunan, penghantaran, dan pelaksanaan aplikasi dalam persekitaran yang terkawal dimana ianya juga turut dikenali sebagai dengan nama kontena. Konsep ini membolehkan pengurusan sumber kod dan pemacu aplikasi. Pengguna boleh menggunakan fail Dockerfile untuk menentukan konfigurasi dan langkah-langkah yang diperlukan untuk membangunkan dan menyediakan aplikasi dalam kontena. Ini membolehkan proses pembangunan dan penghantaran aplikasi dijalankan secara automatik. Terdapat banyak lagi fungsi kontena lainnya, tetapi dalam konteks pembangunan EGV ini kontena digunapakai bagi mempercepat pembuktian integrasi dan pengoperasian perkhidmatan mikro. Setiap perkhidmatan mikro akan dijalankan dalam kontena yang berasingan, dimana ianya membolehkan pemacuan bersih dan pemantauan yang berkesan terhadap setiap komponen aplikasi.

Rangka Kerja Front End / Back End

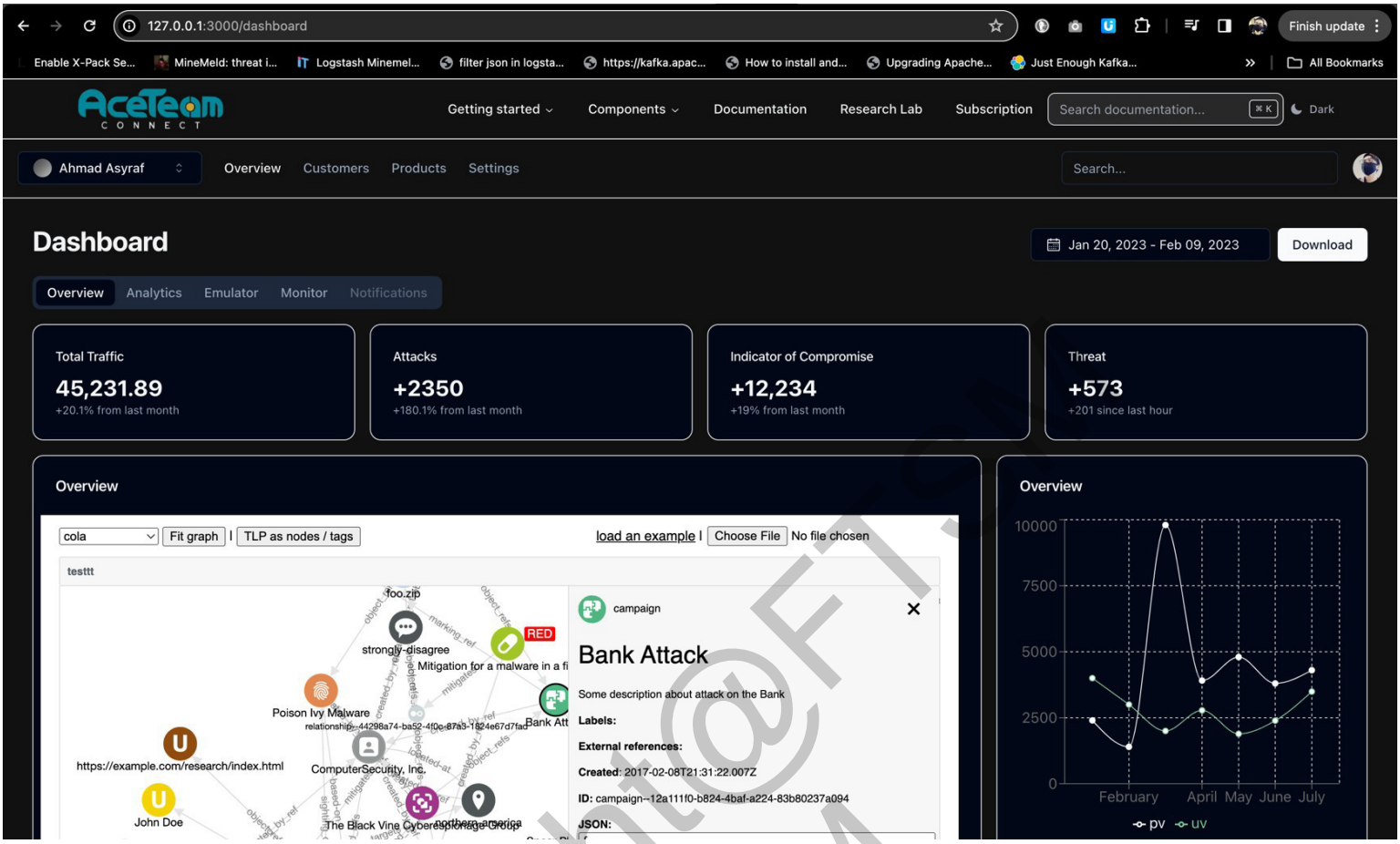
Sejurus lengkapnya penyediaan persekitaran I-III, setiap perkara dalam senarai rangka kerja akan dikonfigurasi pada persekitaran yang telah tersedia mengikut seperti perancangan yang telah dinyatakan dalam usulan. Sebagai contoh, antaranya termasuklah dan tidak terhad kepada Django dan NextJs. Merujuk kepada senarai rangka kerja yang telah dirancang, terdapat banyak lagi perincian komponen yang akan digunakan sepanjang pembangunan solusi EGV ini. antaranya termasuklah Tailwind, Mitre, Shadcn dan sebagainya. Antara dasar penggunaan rangka kerja berikut adalah disebabkan oleh kemudahan yang tersedia berlandaskan bahasa perngaturcaraan, penggunaan rangka kerja akan lebih menjimatkan tempoh waktu, meningkatkan produktiviti serta memudahkan proses pembangunan berbanding dengan pendekatan secara kaedah vanilla (manual).

Pangkalan Data

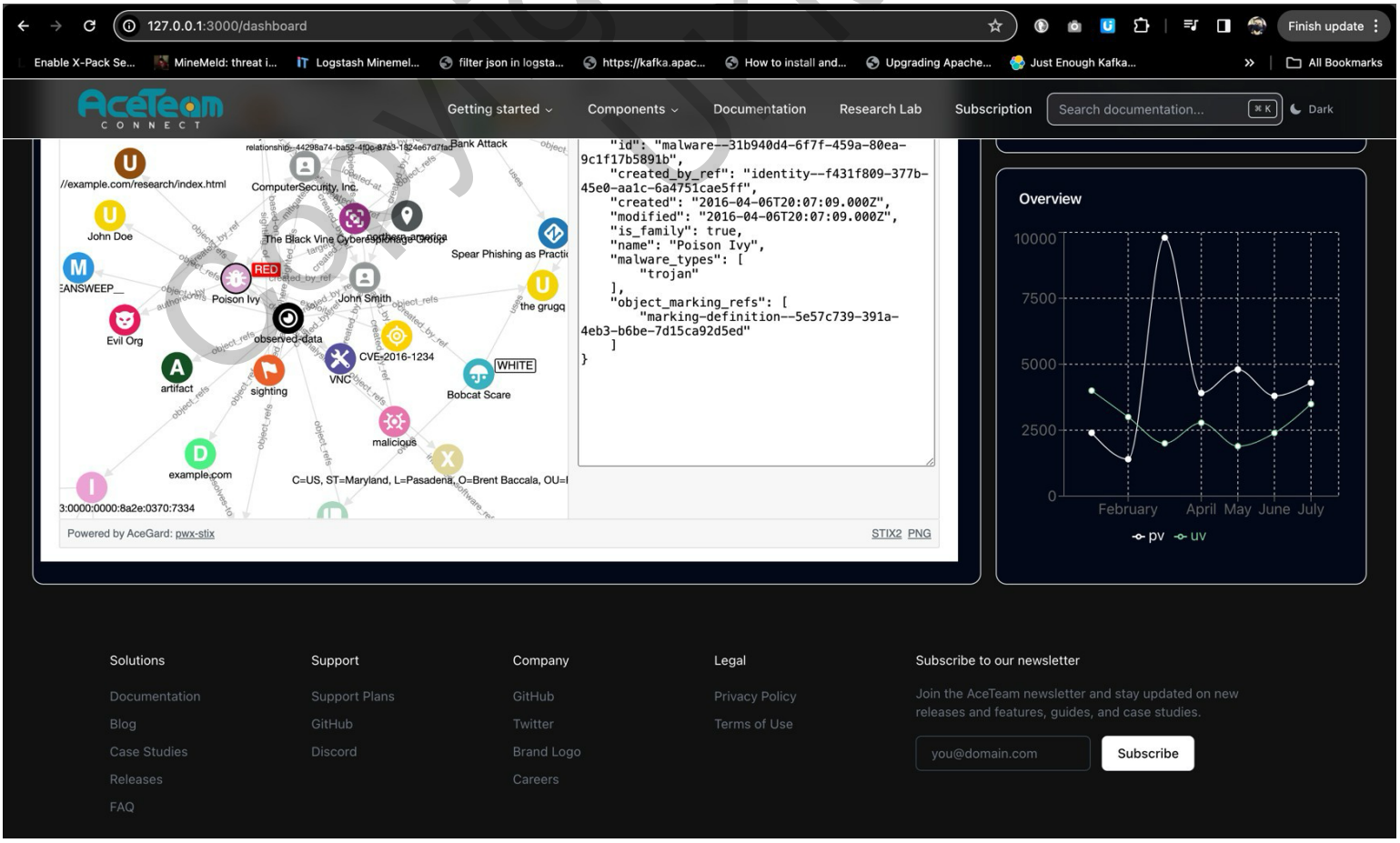
Dalam pembangunan solusi EGV ini, terdapat beberapa jenis pangkalan data yang akan digunapakai, terutamanya pangkalan data dengan jenis NoSQL bagi memudahkan penyimpanan dan pencarian sebarang data yang berstruktur mahupun tidak berstruktur berdasarkan kata kekunci utama, antara pangkalan data yang digunakan adalah memcache, elasticsearch dan sebagainya. konsep transaksi berpandukan kata kekunci ini adalah untuk memudahkan status sesuatu data itu dikemaskini secara berturutan ataupun serentak tanpa perlu menggunakan sumber pengkomputeran yang tinggi bagi proses pertanyaan "query" yang rumit. Hal ini kerana rekod yang disimpan dapat diperoleh dan dikemaskini (seperti kes guna model peluruhan) menerusi kata kekunci yang unik. Tambahan pula, segala operasi yang memerlukan sumber yang tinggi dapat diperuntukkan kepada proses penghuraian, transformasi dan korelasi maklumat

Perkhidmatan Terurus

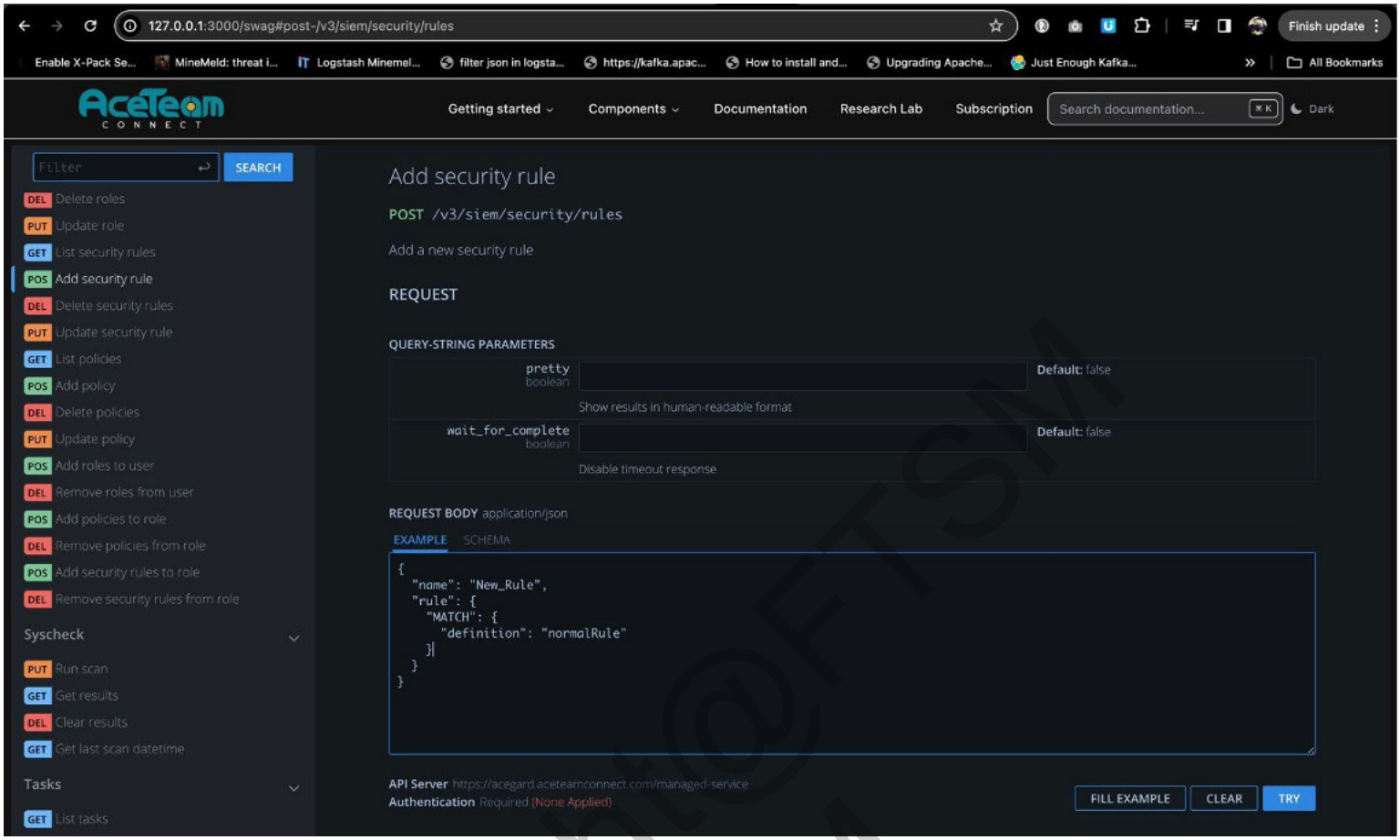
Persekitaran terdahulu yang telah dikonfigurasi akan dihimpunkan di bawah perisian berpusat bagi memudahkan pengelolaan dan pengendalian sepanjang proses pembangunan berlangsung. Perisian berpusat ini menyediakan platform yang konsisten dan seragam, membolehkan setiap komponen persekitaran diurus dengan lebih efisyen dan teratur. Melalui pendekatan ini, pasukan pembangunan dapat memastikan kesemua tetapan persekitaran adalah selaras dengan keperluan projek, mengurangkan risiko ketidakselarasan dan kesilapan yang boleh berlaku semasa pembangunan. Perisian berpusat ini juga menawarkan kemudahan automasi dalam pengurusan persekitaran, termasuk pengemaskinian perisian, pemantauan prestasi, dan pengurusan sumber. Automasi ini dapat menjimatkan masa dan usaha pasukan, di mana ianya membolehkan mereka fokus kepada tugas-tugas yang lebih kritikal dan bernilai tambah. Di samping itu, perisian ini juga membolehkan pemantauan yang lebih menyeluruh dan berkesan, di mana setiap perubahan dan prestasi persekitaran dapat dipantau secara masa nyata.



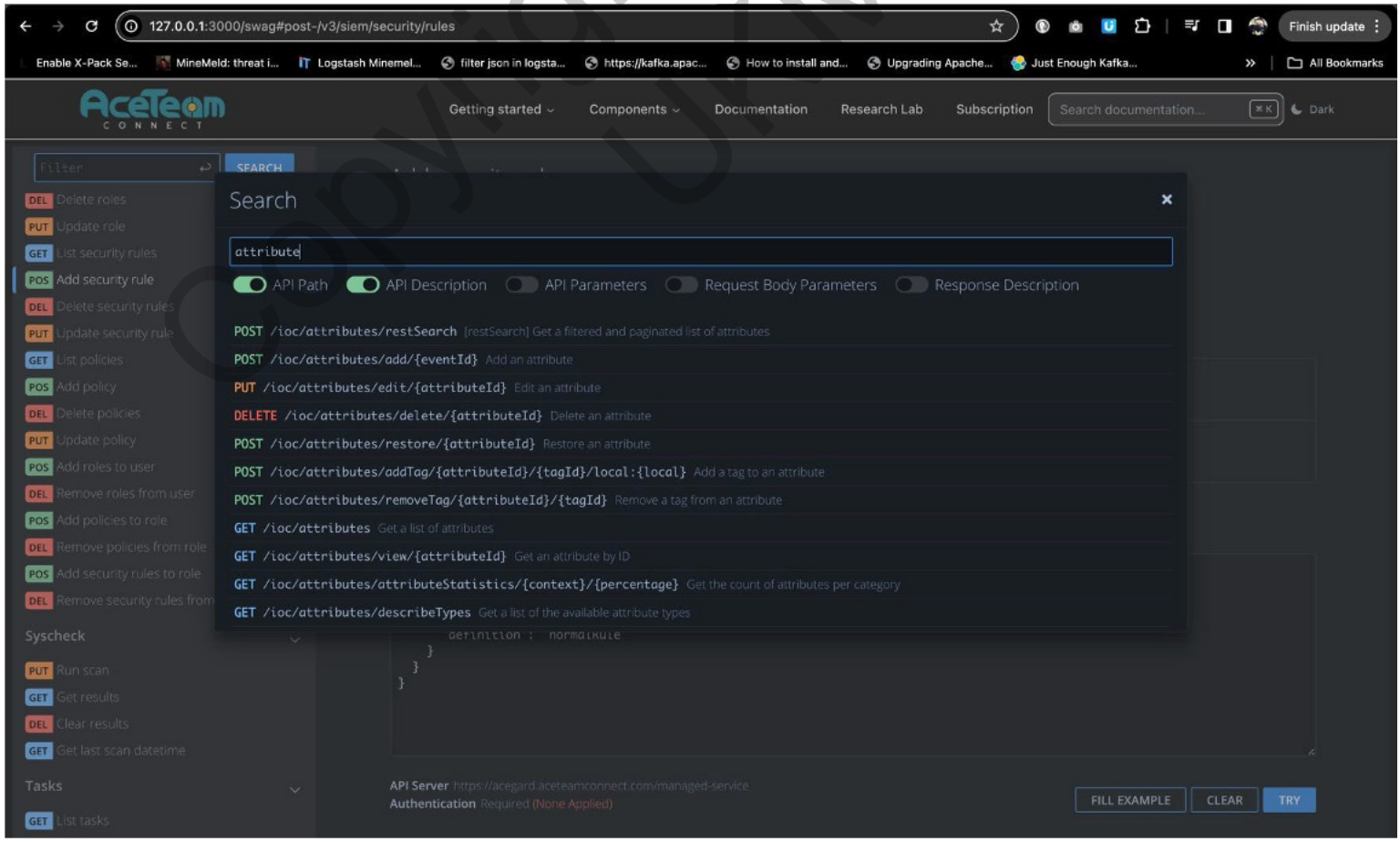
Rajah 1.0 Antara muka halaman utama EGV



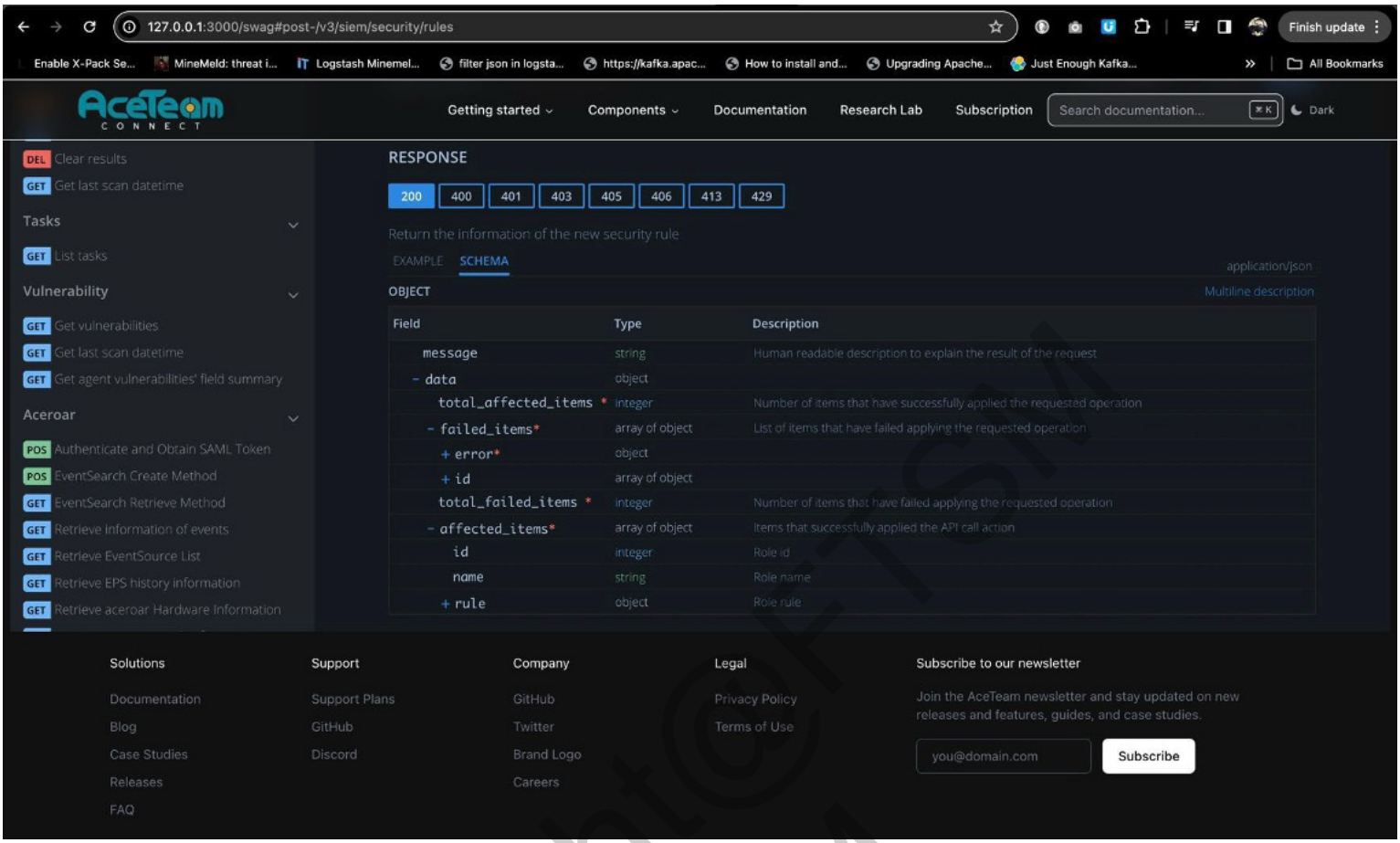
Rajah 2.0 Antara muka footer EGV



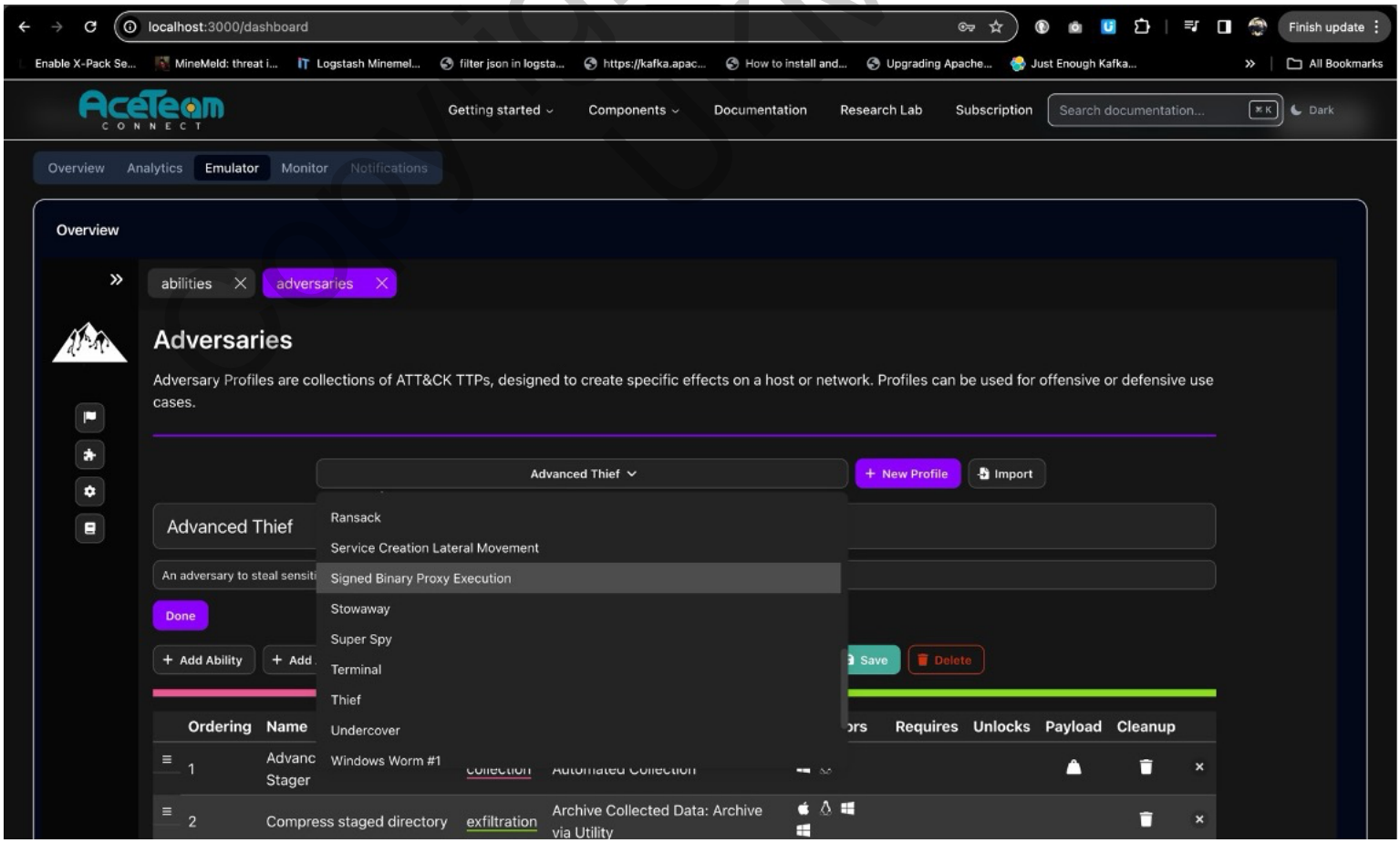
Rajah 3.0 Antara muka spesifikasi API



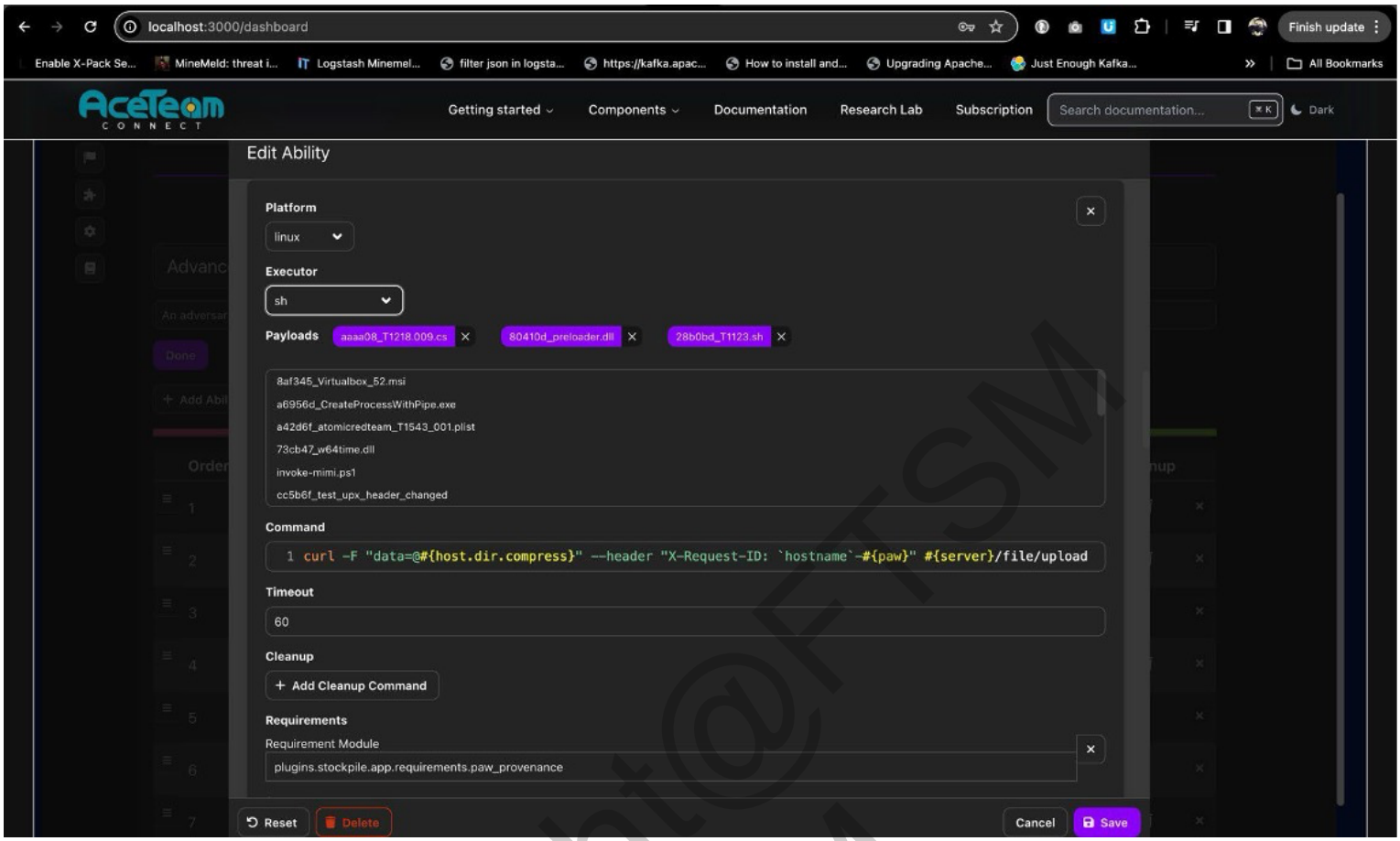
Rajah 4.0 Antara muka saringan lanjutan



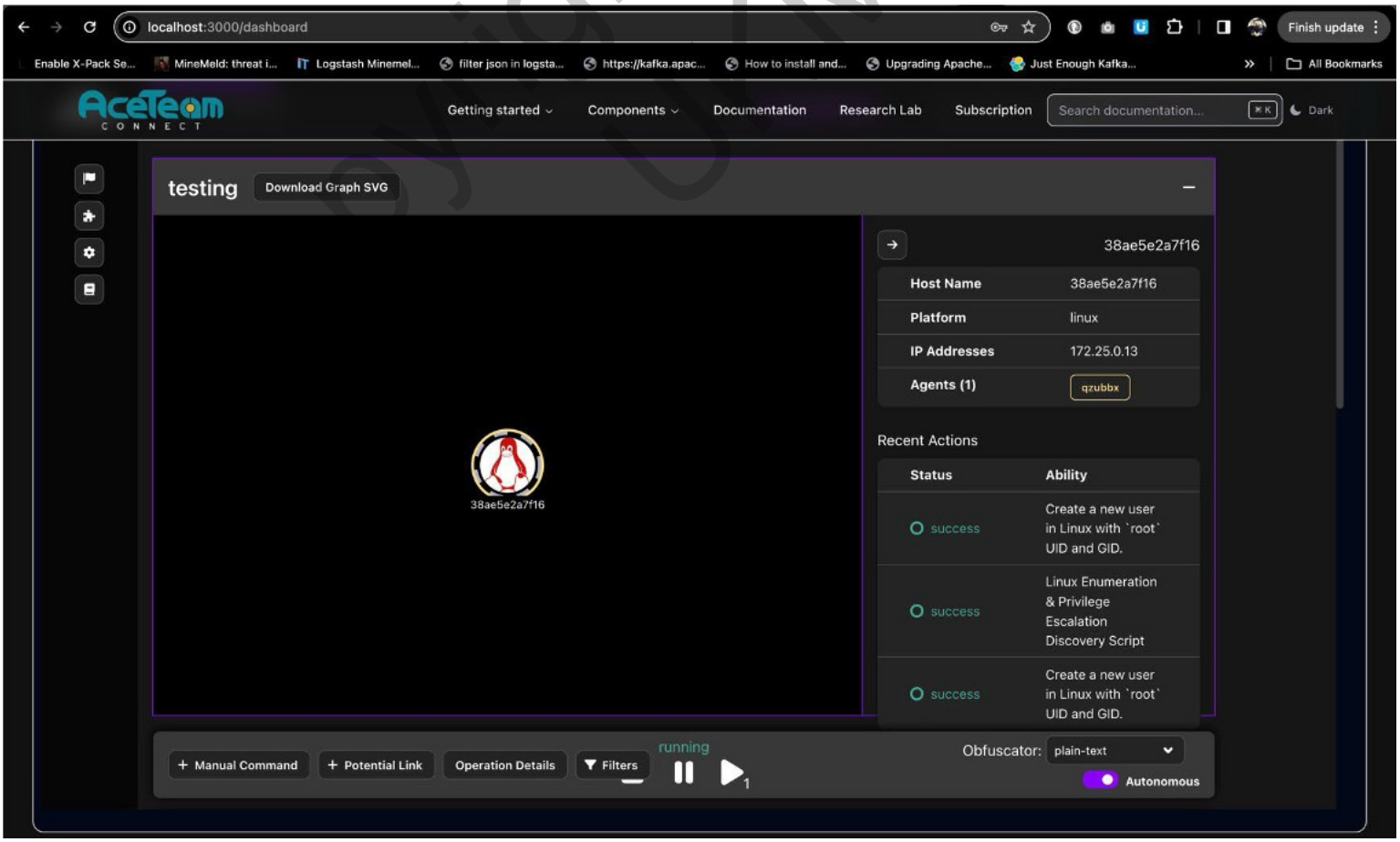
Rajah 5.0 Antara muka laman interaktif



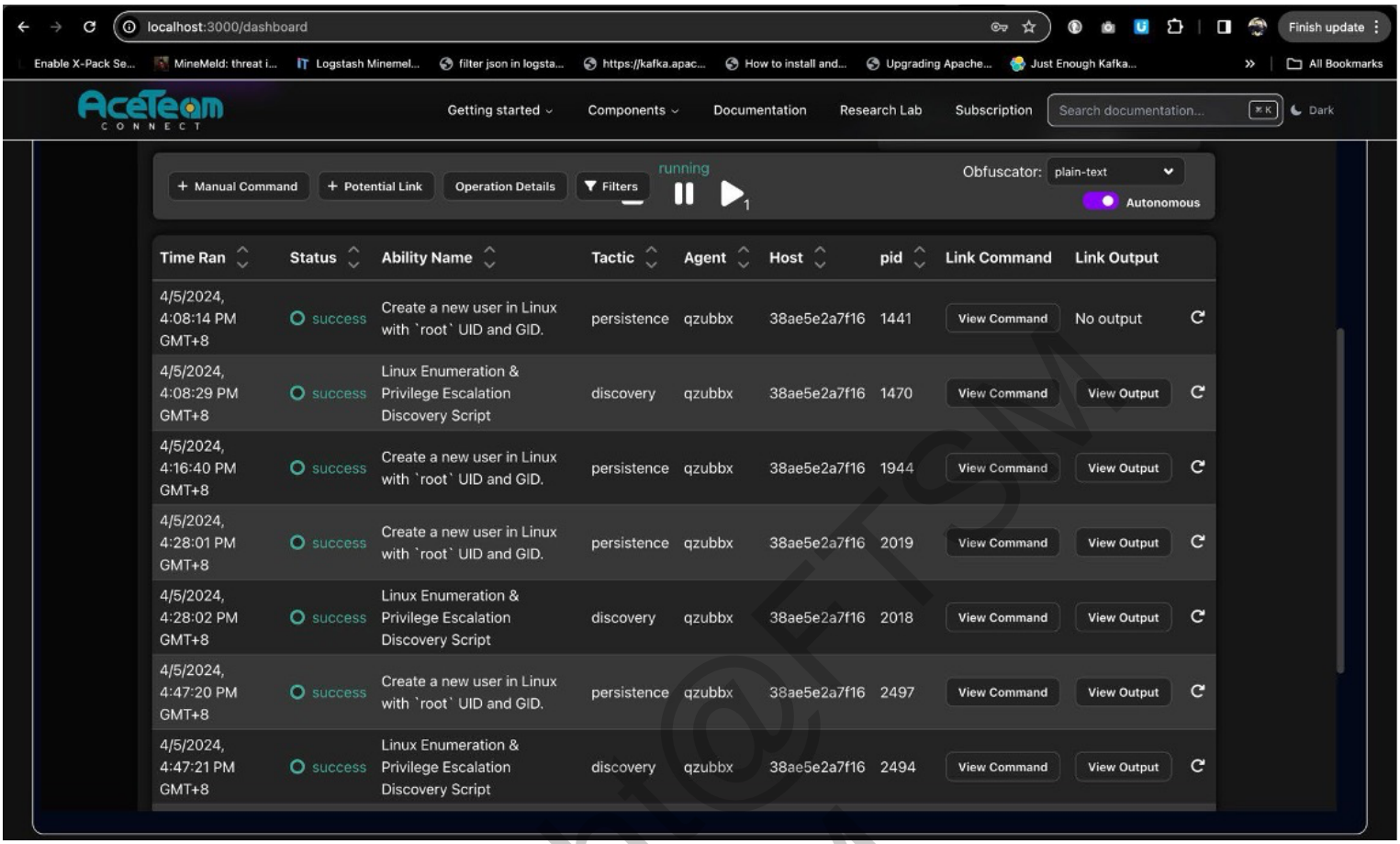
Rajah 6.0 Antara muka simulasi serangan



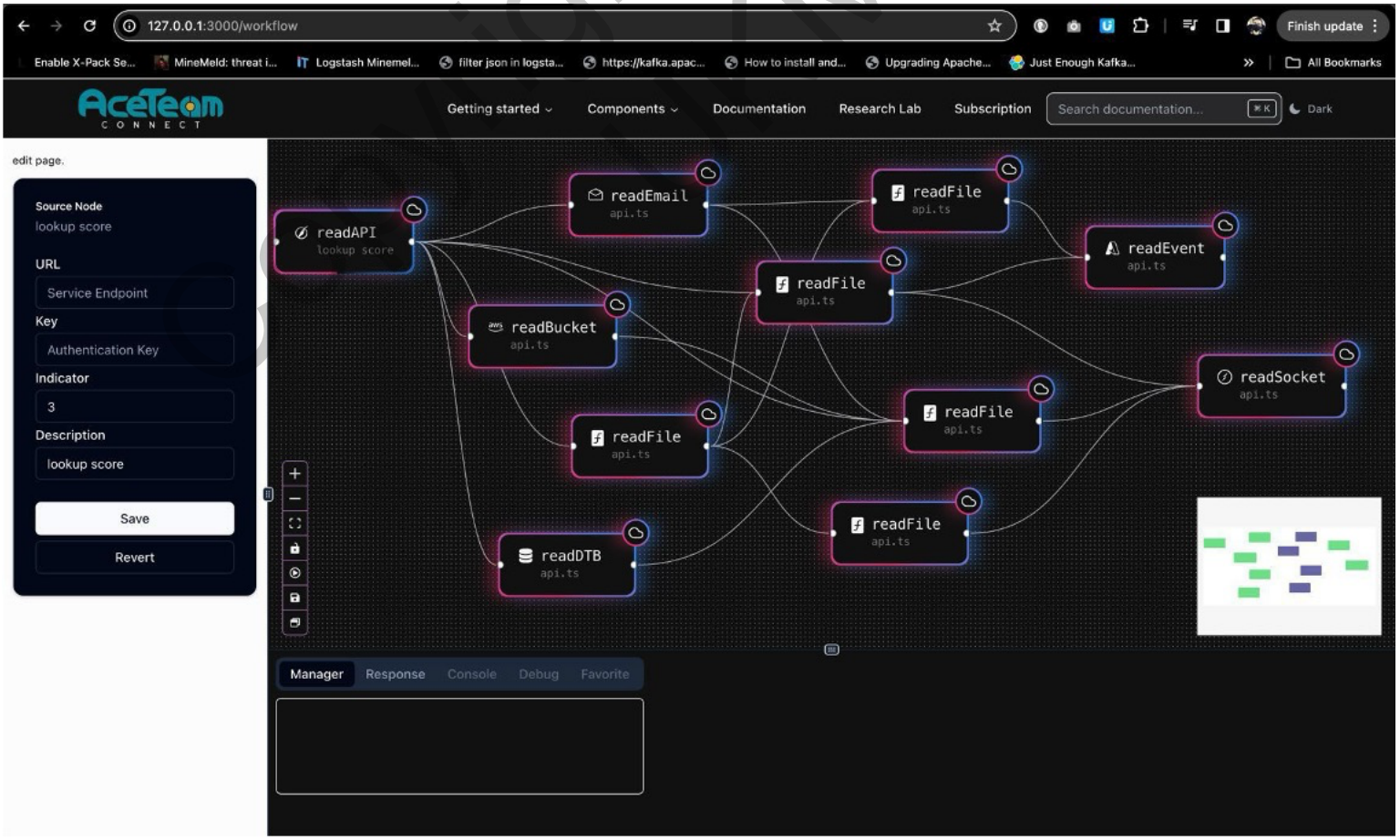
Rajah 7.0 Antara muka penyeseuain serangan (payload)



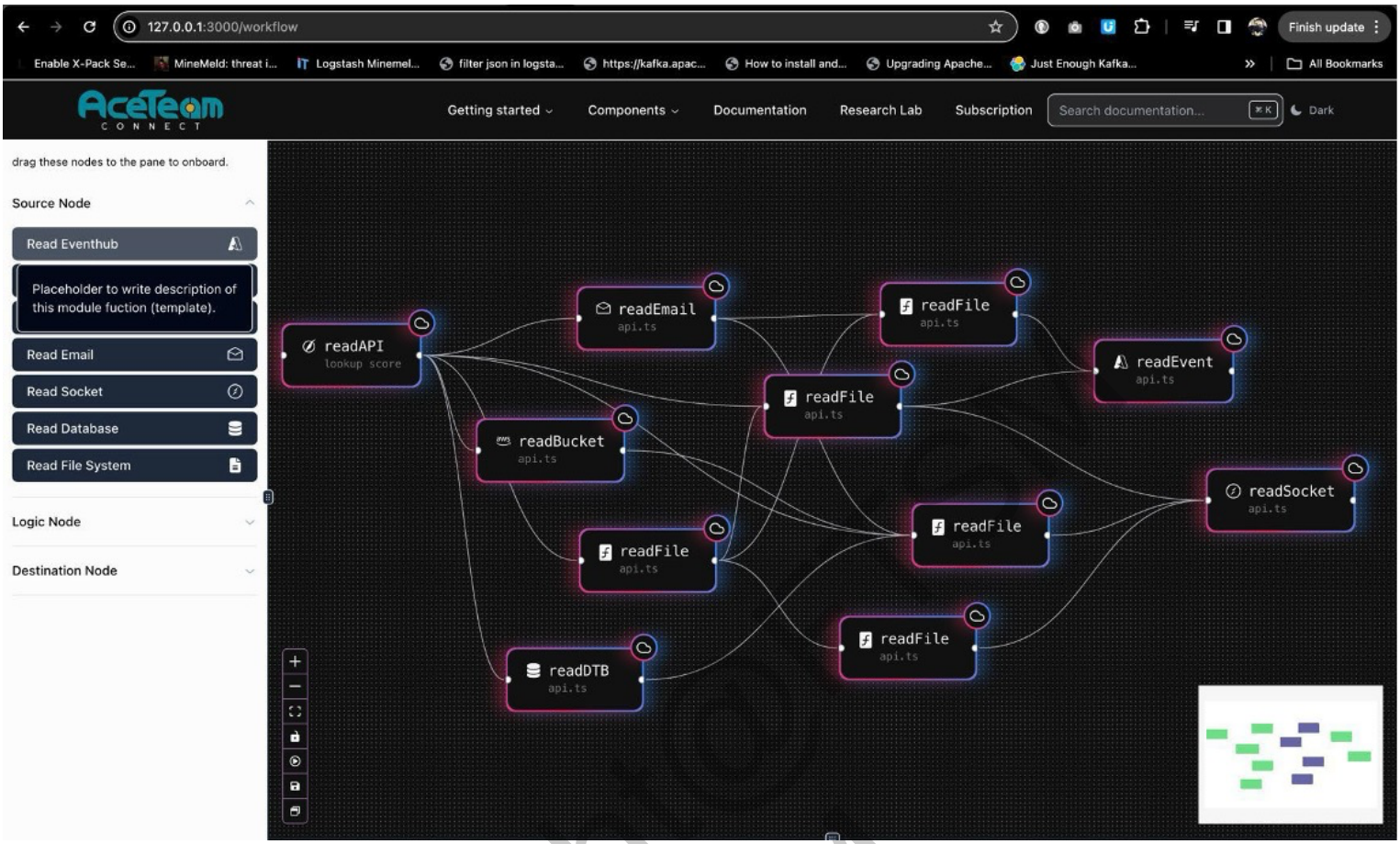
Rajah 8.0 Antara muka halaman impak serangan



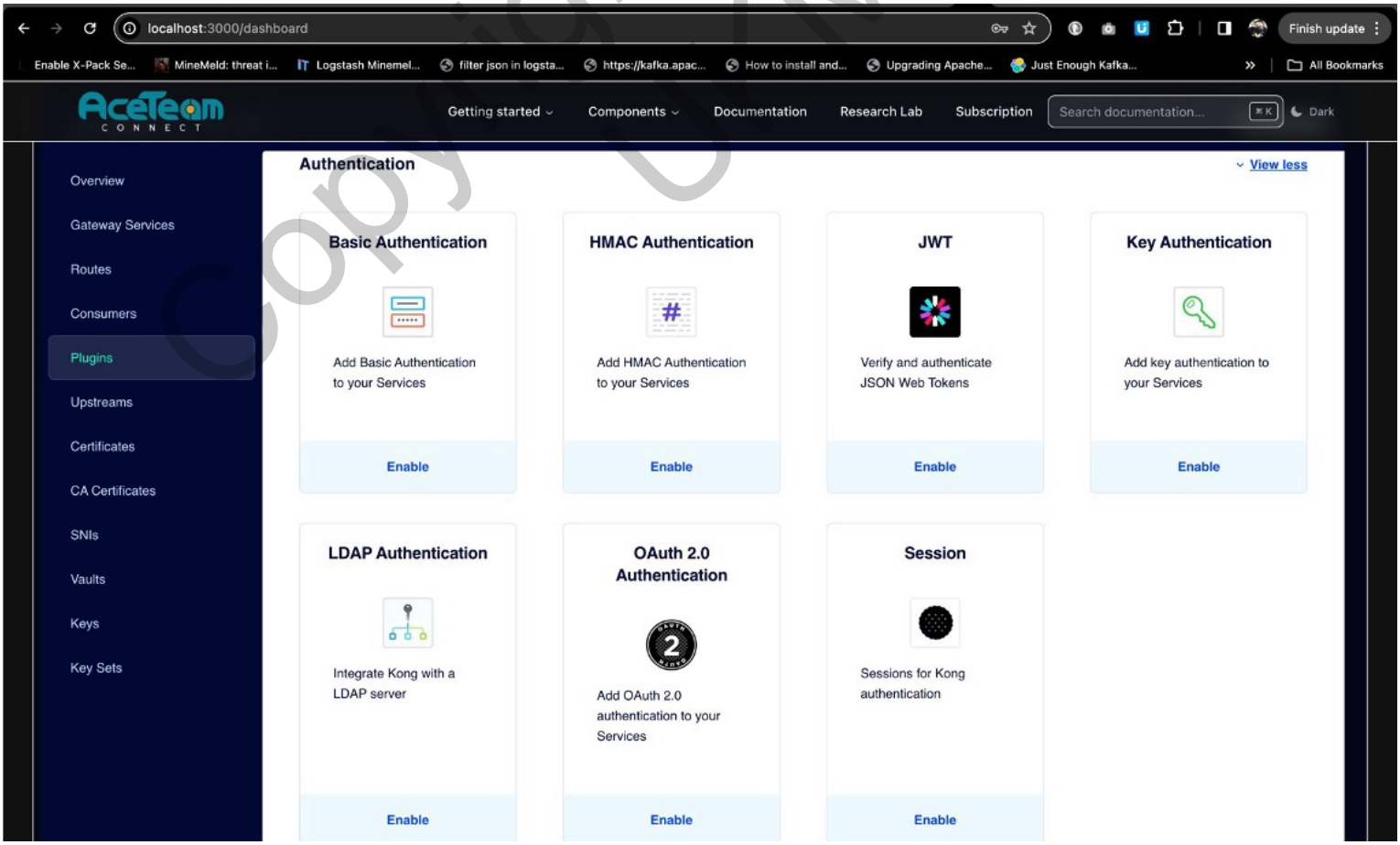
Rajah 9.0 Antara muka status historikal serangan



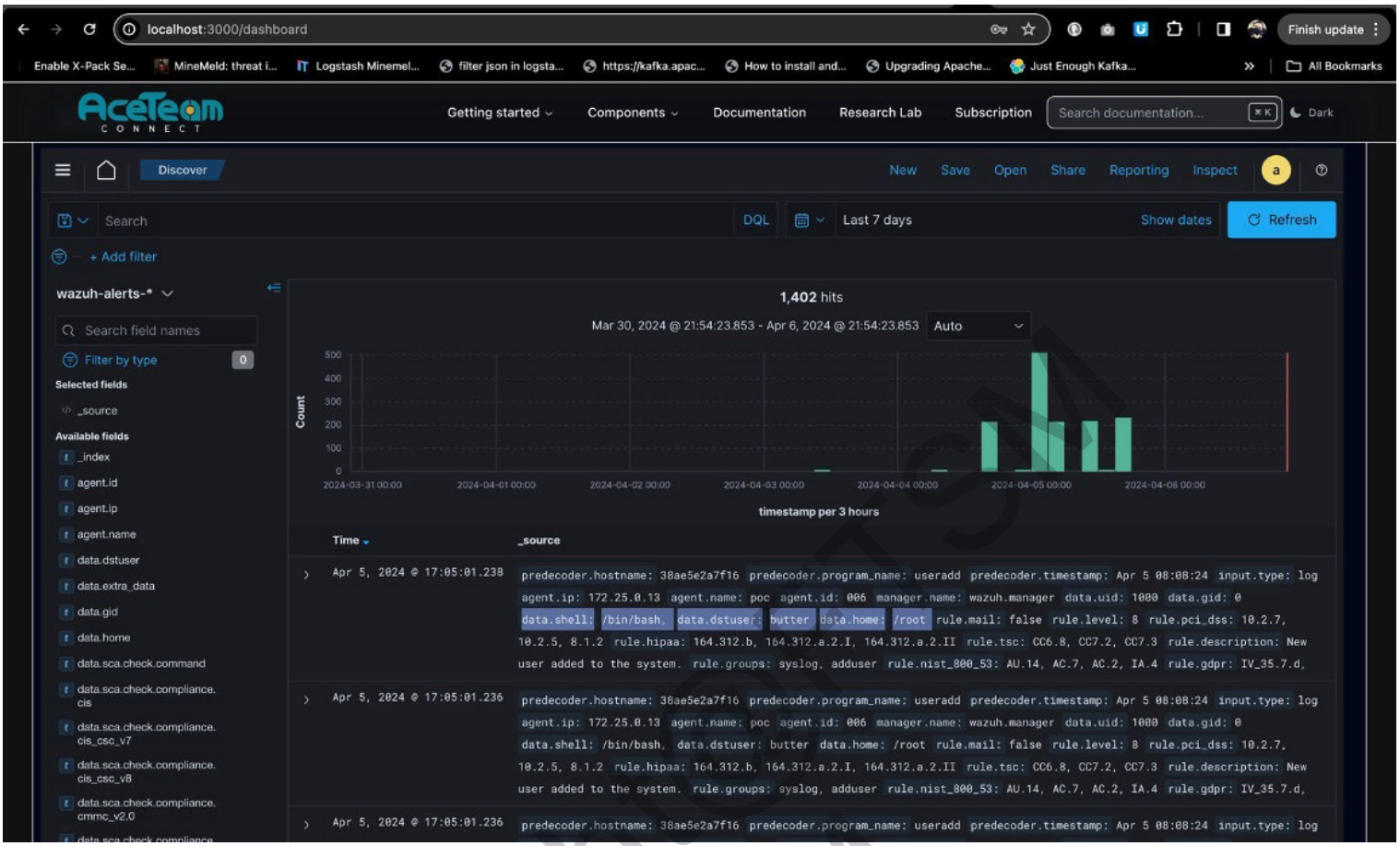
Rajah 10.0 Antara muka orkestrasi alur kerja bersyarat



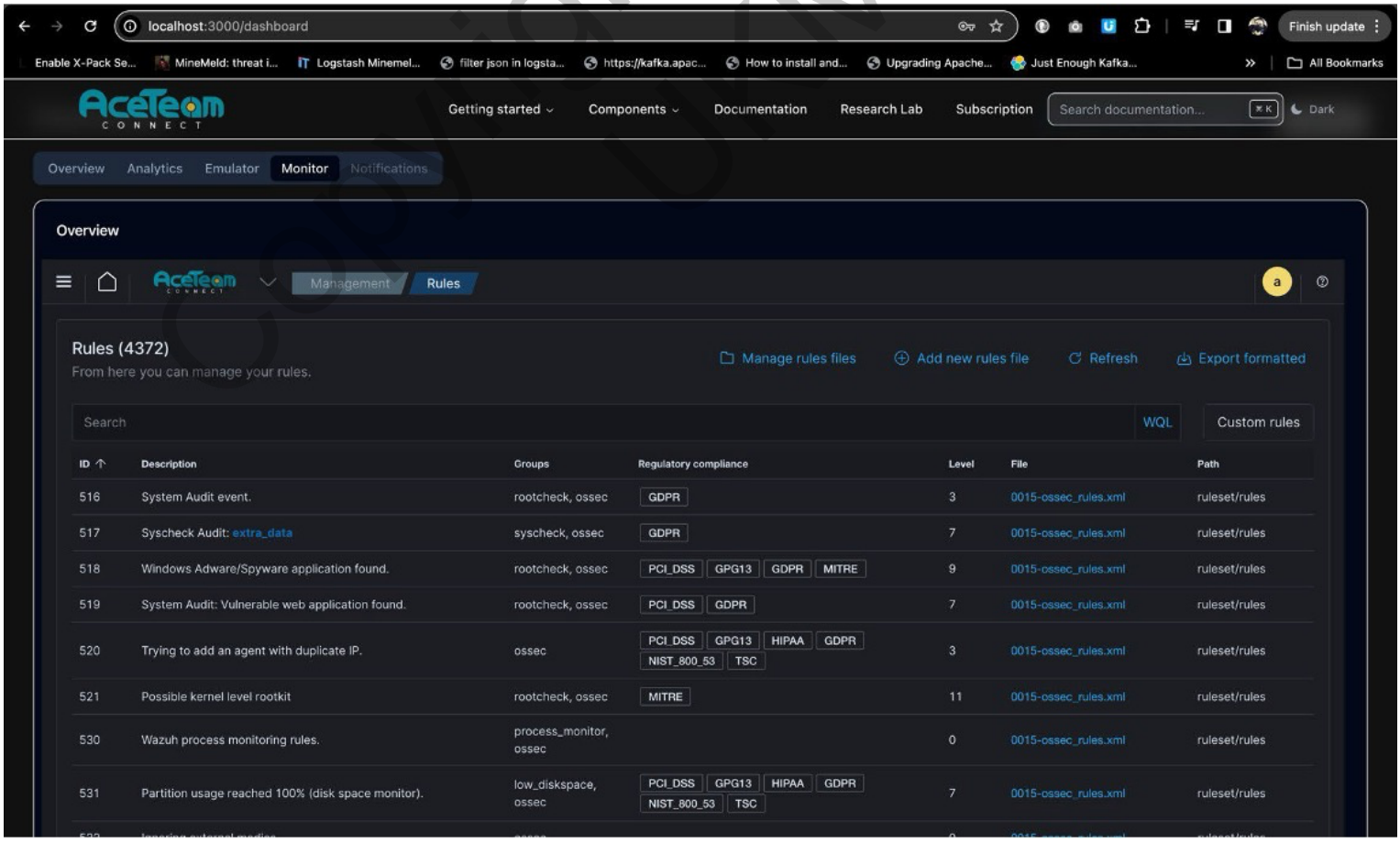
Rajah 11.0 Antara muka sumber integrasi orkestrasi



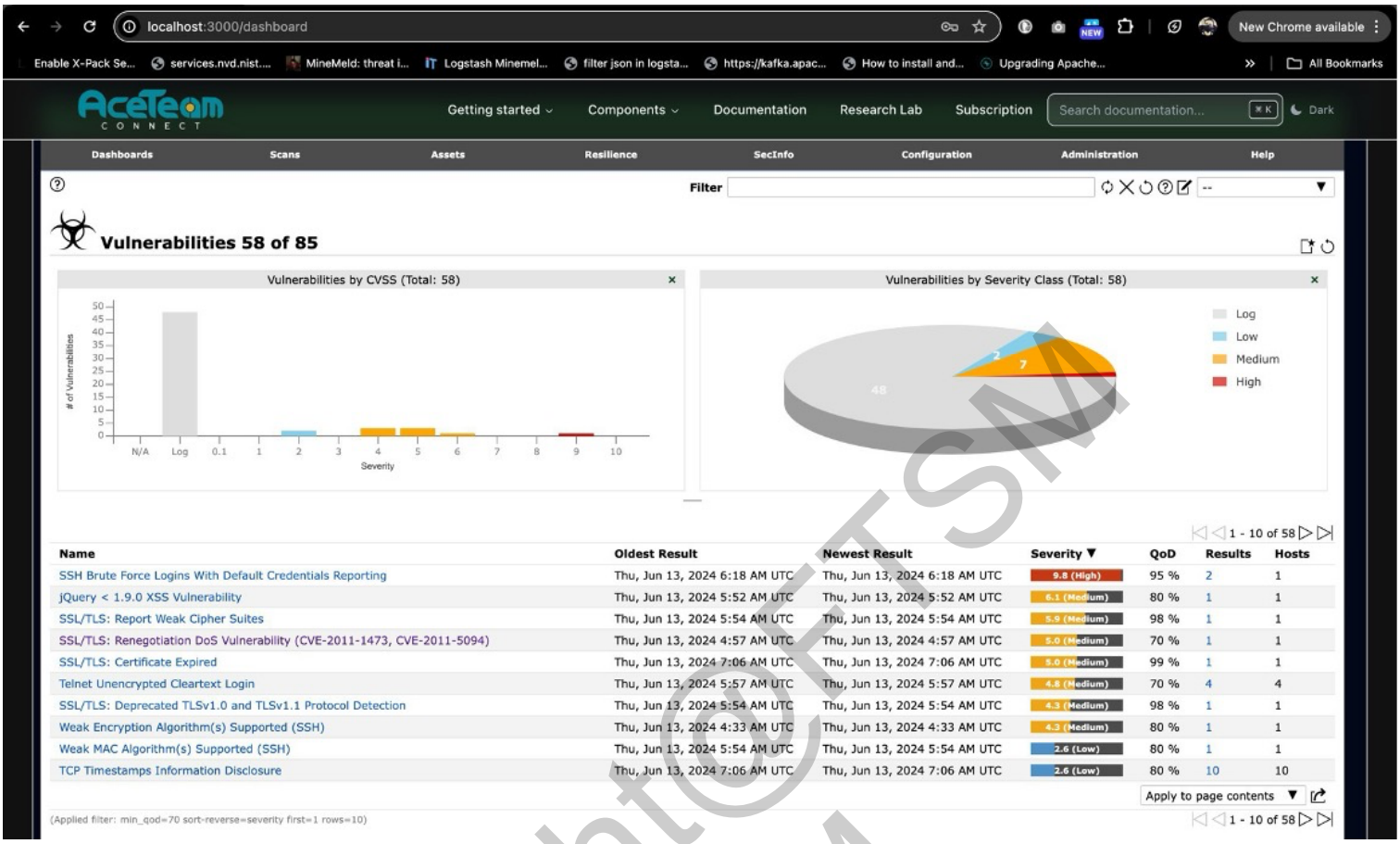
Rajah 12.0 Antara muka pengesahan identiti



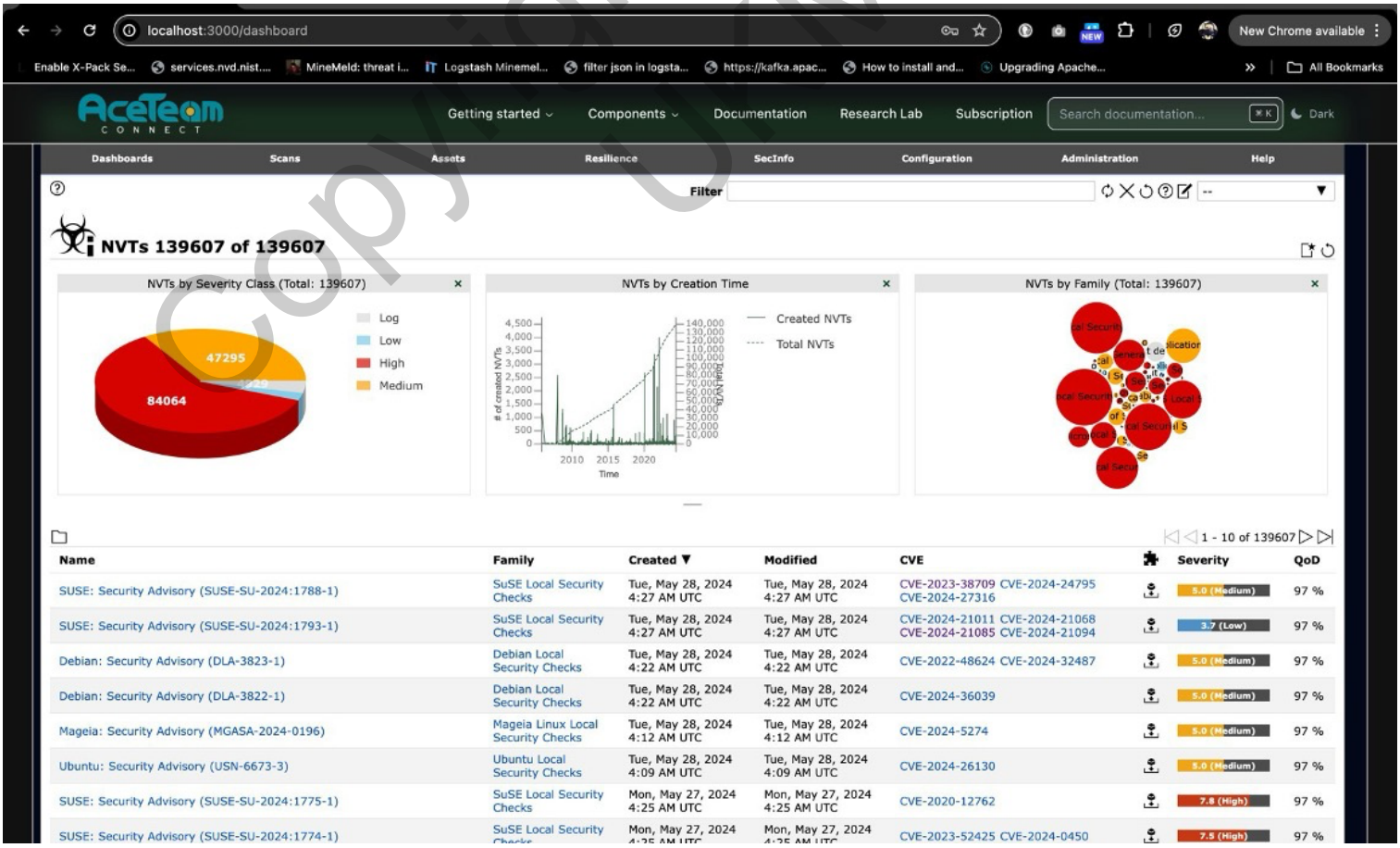
Rajah 13.0 Antara muka pemaparan data yang telah dihuraikan



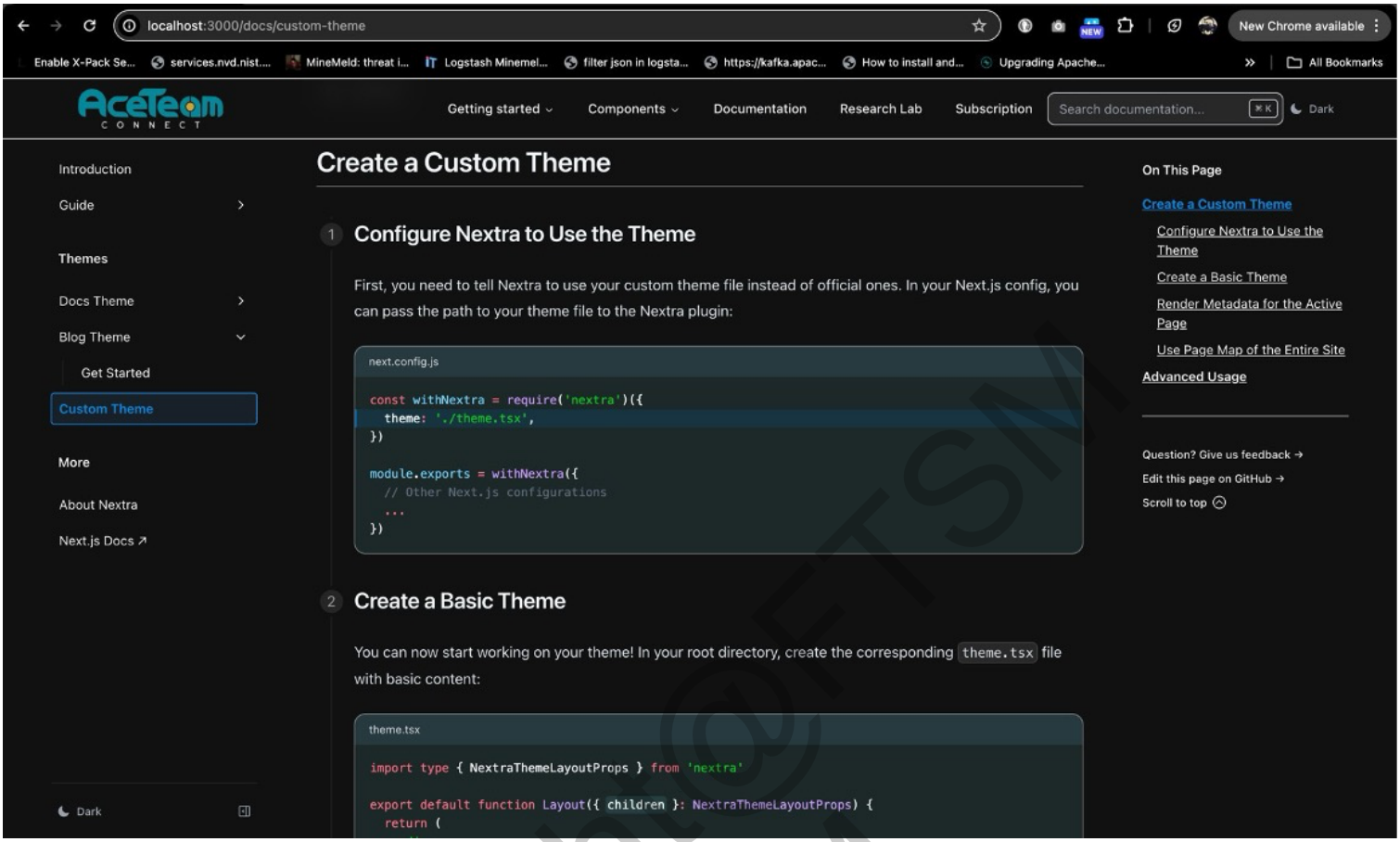
Rajah 14.0 Antara muka perincian petua bagi sistem pengesan pencorobohan



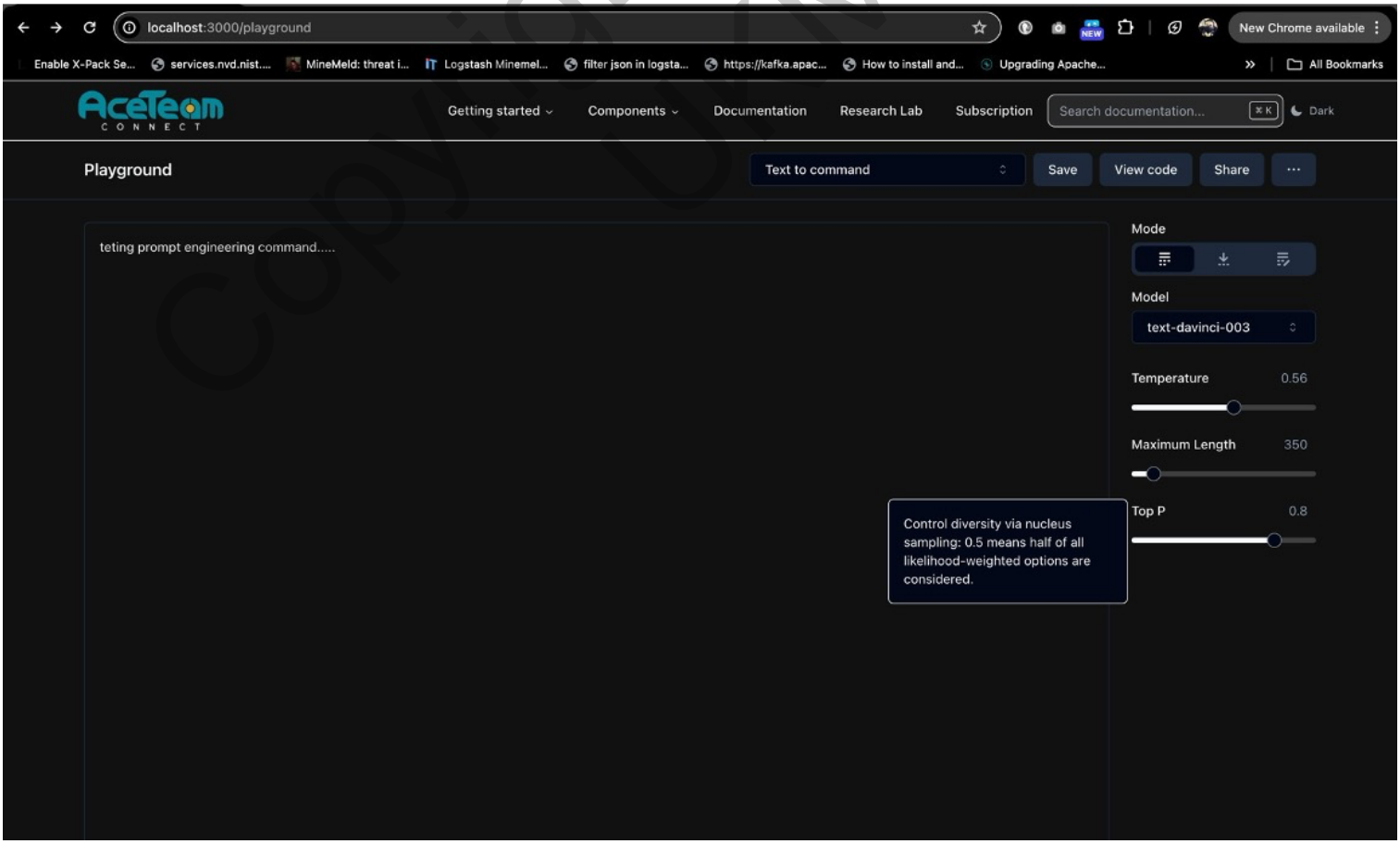
Rajah 15.0 Antara muka halaman penilaian risiko serangan



Rajah 16.0 Antara muka profail serangan



Rajah 17.0 Antara muka ruangan pengetahuan berpusat



Rajah 18.0 Antara muka ruangan penambahbaikan model

Platform perkhidmatan terurus EGV ini memainkan peranan penting dalam membantu organisasi mengenal pasti, menganalisis, dan bertindak balas terhadap ancaman siber. Latar belakang kajian ini bermula dengan keperluan untuk meningkatkan keupayaan CTI melalui pembelajaran berterusan, yang bertujuan untuk memperbaiki kualiti, mengembangkan kepelbagaian korelasi dan meningkatkan ketepatan maklumat ancaman yang diterima daripada sensor mahupun pencegah pencerobohan. Manakala dari perspektif produktiviti dan efisyensi pula, alur kerja orkestrasi juga memberikan impak yang besar dalam operasi sehari- harian. Objektif utama ujian ini adalah untuk menilai keberkesanan dan kebolehgunaan sistem EGV secara menyeluruh. Ini termasuk dan tidak terhad kepada komponen selingan (integrasi) serta modul sampingan yang terkandung dalam platform EGV ini.

Objektif pengujian telah dilaksanakan bagi:

- Memastikan bahawa setiap unit komponen dalam sistem yang memiliki fungsi serta peranan yang berbeza dapat saling berkomunikasi dan beroperasi bersama secara efisyen.
- Memastikan seluruh sistem diuji secara menyeluruh untuk memastikan ianya memenuhi semua keperluan yang telah ditetapkan dalam menjalankan fungsi.
- Memastikan ujian penerimaan dilaksanakan bersama pengguna dan pihak berkepentingan untuk memastikan sistem sesuai dengan jangkaan.

Susun atur kajian ujian ini merangkumi ujian kebolehgunaan, ujian prestasi, dan ujian ketepatan maklumat ancaman. Instrumen yang digunakan termasuk perisian simulasi ancaman siber untuk menguji maklumbalas sistem serta soal selidik untuk mendapatkan maklum balas pengguna. Prosedur ujian melibatkan beberapa langkah, seperti persediaan ujian, pelaksanaan ujian, dan analisis hasil ujian. Kempulan sampel terdiri daripada pakar keselamatan siber dan pengguna akhir untuk mendapatkan pandangan yang pelbagai dari segenap sudut mengenai keberkesanan solusi. Data yang telah dikumpulkan akan dianalisis menggunakan kaedah statistik dan pembelajaran mesin secara berterusan untuk menilai prestasi sistem. Pengumpulan data melibatkan rekod aktiviti sistem, respon terhadap ancaman, dan maklum balas pengguna mengenai kebolehgunaan dan ketepatan maklumat ancaman.

Hasil ujian menunjukkan bahawa sistem EGV berasaskan pembelajaran berterusan ini berjaya meningkatkan produktiviti dan keberkesanan analisa dalam mengenal pasti dan menganalisis ancaman siber. Penyampaian visual yang diperoleh dalam bentuk nod dan graf

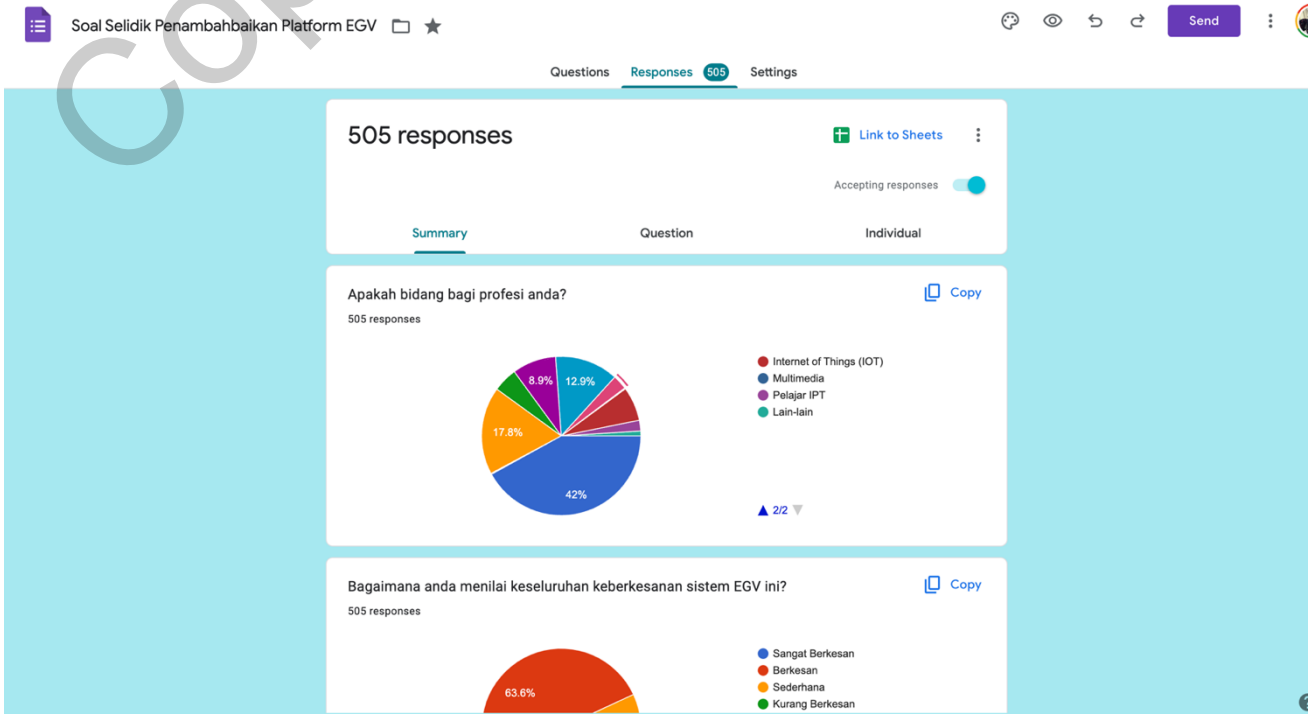
membolehkan layar maklumat ancamn dapat difahami dengan lebih mudah sekaligus menggambarkan prestasi sistem, ketepatan maklumat ancaman, dan kepuasan pengguna. Analisis hasil menunjukkan bahawa sistem ini berupaya memberikan maklumat ancaman yang tepat dan relevan serta mudah digunakan oleh pengguna. Perbincangan mengenai hasil ujian menunjukkan bahawa terdapat beberapa aspek yang perlu diperbaiki, seperti penyesuaian algoritma pembelajaran mesin dan peningkatan antaramuka pengguna.

Jadual 4.0 Keputusan pengujian fungsian

ID Pelan Ujian	Nama Pelan Ujian	Objektif Pelan Ujian	ID Fungsi	Status Penerimaan
PU001	Pengujian fungsi pengesahan identiti	pengguna dapat melakukan proses bagi pengesahan identiti	KF1.1-1.10	Lengkap
PU002	Pengujian fungsi aturan persisten	pengguna dapat menggunakan modul aturan persisten	KF2.1-2.7	Memenuhi
PU003	Pengujian fungsi saringan maklumat	pengguna dapat melakukan saringan maklumat	KF3.1-3.7	Lengkap
PU004	Pengujian fungsi korelasi maklumat	pengguna dapat menjalankan korelasi maklumat dari intel	KF4.1-4.6	Lengkap
PU005	Pengujian fungsi normalisasi data	pengguna dapat menjalankan proses normalisasi data	KF5.1-5.5	Memenuhi
PU006	Pengujian fungsi visualisasi data	pengguna dapat menggunakan modul visualisasi data	KF6.1-6.6	Lengkap
PU007	Pengujian fungsi pengemaskinian hayat	pengguna dapat menggunakan proses pengemaskinian hayat	KF7.1-7.3	Lengkap
PU008	Pengujian fungsi manual berpusat	pengguna mendapatkan faedah dari manual berpusat	KF8.1-1.8.3	Lengkap
PU009	Pengujian fungsi penghapusan dan pengambilan data	pengguna melakukan operasi penghapusan dan pengambilan data	KF9.1-9.4	Lengkap
PU010	Pengujian fungsi pengendalian relevansi	pengguna dapat menggunakan modul pengendalian relevansi	KF10.1-10.5	Lengkap
PU011	Pengujian fungsi pengembangan integrasi	pengguna dapat melakukan pengembangan integrasi	KF11.1-11.5	Lengkap
PU012	Pengujian fungsi perkhidmatan terurus	pengguna dapat menikmati perkhidmatan yang terurus	KF12.1-12.8	Lengkap
PU013	Pengujian fungsi pembelajaran berterusan	pengguna dapat menambahbaik model pebelajaran berterusan	KF13.1-13.7	Memenuhi

PU014	Pengujian fungsi alur kerja bersyarat	pengguna dapat melakukan operasi orkestrasi dan automasi	KF14.1-14.10	Lengkap

Ujian penerimaan pengguna telah dibuat secara berskala berawal daripada ruangan pejabat AceTeam dimana penggunanya terdiri daripada analisa dan jurutera AceTeam sendiri. Ujian ini kemudiannya dibesarkan skopnya kepada pelawat luar yang hadir untuk melawat pusat operasi AceTeam dan dari situ, setiap maklumbalas yang diperoleh akan diambil maklum dan dimasukkan kedalam pelan penambahbaikan berterusan. Tambahan lagi, ujian ini juga turut dilakukan terhadap agensi-agensi kerajaan dan juga swasta yang ahli dalam bidang keselamatan siber ini yang mana rata-rata menunjukkan minat dalam modul dan fungsi yang dibina dalam membantu penyiasatan operasi siber berjalan dengan lebih efisyen dan efektif. Ujian ini juga giat dikendalikan di majlis-majlis yang ditaja oleh AceTeam seperti di UKM sendiri dan bengkel di Cyberjaya, di mana ianya mendapat sambutan dari kalangan ilmuan dan juga ahli bidang kerana ianya merupakan suatu anjakan paradigma terhadap pembaharuan teknologi sedia ada. Bagi ujian kebolehgunaan teknikal, seramai **7 orang responden** telah dipilih terdiri daripada kalangan jurutera keselamatan maklumat, analisa keselamatan maklumat dan juga jurutera R&D. Keputusan menunjukkan bahawa hampir keseluruhan modul telah diuji dengan kriteria lengkap **100%** manakala 3 modul iaitu **PU002**, **PU005** dan **PU013** hanya diuji dengan kriteria sekadar memenuhi objektif kajian **(55% - 70%)** , hal ini berlaku atas dasar kekangan yang telah dinyatakan dalam seksyen sebelum ini. Manakala bagi responden dari soal selidik pula membuahkan maklumbalas daripada 505 responden yang terdiri dari pelbagai latar profesi.



		Q1					
		Berkesan		Sangat Berkesan		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	10	66.67%	4	26.67%	1	6.67%
	Internet of Things (IOT)	24	68.57%	8	22.86%	3	8.57%
	IT Konsultan (GRC)	31	68.89%	13	28.89%	1	2.22%
	Kecerdasan Buatan	15	60.00%	10	40.00%	0	0.00%
	Keselamatan Siber	136	64.15%	58	27.36%	18	8.49%
	Lain-lain	4	80.00%	1	20.00%	0	0.00%
	Pelajar IPT	7	63.64%	2	18.18%	2	18.18%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	0	0.00%	1	100.00%	0	0.00%
	Pengkomputeran Awan	40	61.54%	23	35.38	2	3.08
	Sistem Rangkaian	54	60.00%	28	31.11%	8	8.89%

		Q2			
		Membantu		Sangat Membantu	
		Count	Row N %	Count	Row N %
PROFESI	Data Sains	3	20.00%	12	80.00%
	Internet of Things (IOT)	13	37.14%	22	62.86%
	IT Konsultan (GRC)	14	31.11%	31	68.89%
	Kecerdasan Buatan	5	20.00%	20	80.00%
	Keselamatan Siber	44	20.75%	168	79.25%
	Lain-lain	1	20.00%	4	80.00%
	Pelajar IPT	3	27.27%	8	72.73%
	Pembantu Teknikal	0	0.00%	1	100.00%
	Pengaturcaraan	1	100.00%	0	0.00%
	Pengkomputeran Awan	11	16.92%	54	83.08%
	Sistem Rangkaian	16	17.78%	74	82.22%

		Q3					
		Memuaskan		Sangat Memuaskan		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	13	86.67%	2	13.33%	0	0.00%
	Internet of Things (IOT)	33	94.29%	1	2.86%	1	2.86%
	IT Konsultan (GRC)	31	68.89%	10	22.22%	4	8.89%
	Kecerdasan Buatan	18	72.00%	6	24.00%	1	4.00%
	Keselamatan Siber	172	81.13%	31	14.62%	9	4.25%
	Lain-lain	4	80.00%	1	20.00%	0	0.00%
	Pelajar IPT	8	72.73%	3	27.27%	0	0.00%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	0	0.00%	1	100.00%	0	0.00%
	Pengkomputeran Awan	54	83.08%	6	09.23%	5	7.69%
	Sistem Rangkaian	78	86.67%	7	7.78%	5	5.56%

		Q4			
		Membantu		Sangat Membantu	
		Count	Row N %	Count	Row N %
PROFESI	Data Sains	2	13.33%	13	86.67%
	Internet of Things (IOT)	2	5.71%	33	94.29%
	IT Konsultan (GRC)	5	11.11%	40	88.89%
	Kecerdasan Buatan	3	12.00%	22	88.00%
	Keselamatan Siber	21	9.91%	191	90.09%
	Lain-lain	2	40.00%	3	60.00%
	Pelajar IPT	1	9.09%	10	90.91%
	Pembantu Teknikal	0	0.00%	1	100.00%
	Pengaturcaraan	1	100.00%	0	0.00%
	Pengkomputeran Awan	11	16.92%	54	0.83.08%
	Sistem Rangkaian	9	10.00%	81	90.00%

		Q5			
		Membantu		Sangat Membantu	
		Count	Row N %	Count	Row N %
PROFESI	Data Sains	2	13.33%	13	86.67%
	Internet of Things (IOT)	9	25.71%	26	74.29%
	IT Konsultan (GRC)	6	13.33%	39	86.67%
	Kecerdasan Buatan	2	8.00%	23	92.00%
	Keselamatan Siber	32	15.09%	180	84.91%
	Lain-lain	0	0.00%	5	100.00%
	Pelajar IPT	1	9.09%	10	90.91%
	Pembantu Teknikal	0	0.00%	1	100.00%
	Pengaturcaraan	1	100.00%	0	0.00%
	Pengkomputeran Awan	8	12.31%	57	87.69%
	Sistem Rangkaian	15	16.67%	75	83.33%

		Q6					
		Agak Mempermudahkan		Sangat Mempermudahkan		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	9	60.00%	5	33.33%	1	6.67%
	Internet of Things (IOT)	19	54.29%	15	42.86%	1	2.86%
	IT Konsultan (GRC)	28	62.22%	17	37.78%	0	0.00%
	Kecerdasan Buatan	12	48.00%	13	52.00%	0	0.00%
	Keselamatan Siber	122	57.55%	82	38.68%	8	3.77%
	Lain-lain	2	40.00%	3	60.00%	0	0.00%
	Pelajar IPT	9	81.82%	2	18.18%	0	0.00%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	0	0.00%	1	100.00%	0	0.00%
	Pengkomputeran Awan	34	52.31	29	44.62	2	3.08%
	Sistem Rangkaian	47	52.22%	40	44.44%	3	3.33%

		Q7					
		Agak Mempermudahkan		Sangat Mempermudahkan		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	11	73.33%	4	26.67%	0	0.00%
	Internet of Things (IOT)	21	60.00%	14	40.00%	0	0.00%
	IT Konsultan (GRC)	28	62.22%	15	33.33%	2	4.44%
	Kecerdasan Buatan	12	48.00%	11	44.00%	2	8.00%
	Keselamatan Siber	142	66.98%	66	31.13%	4	1.89%
	Lain-lain	2	40.00%	3	60.00%	0	0.00%
	Pelajar IPT	7	63.64%	4	36.36%	0	0.00%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	0	0.00%	1	100.00%	0	0.00%
	Pengkomputeran Awan	44	67.69%	20	30.77%	1	1.54%
	Sistem Rangkaian	59	65.56%	30	33.33%	1	1.11%

		Q8					
		Agak Mempermudahkan		Sangat Mempermudahkan		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	8	53.33%	7	46.67%	0	0.00%
	Internet of Things (IOT)	18	51.43%	15	42.86%	2	5.71%
	IT Konsultan (GRC)	17	37.78%	27	60.00%	1	2.22%
	Kecerdasan Buatan	10	40.00%	12	48.00%	3	12.00%
	Keselamatan Siber	91	42.92%	107	50.47%	14	6.60%
	Lain-lain	2	40.00%	3	60.00%	0	0.00%
	Pelajar IPT	3	27.27%	8	72.73%	0	0.00%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	0	0.00%	1	100.00%	0	0.00%
	Pengkomputeran Awan	29	44.62%	32	49.23%	4	6.15%
	Sistem Rangkaian	38	42.22%	46	51.11%	6	6.67%

		Q9			
		Membantu		Sangat Membantu	
		Count	Row N %	Count	Row N %
PROFESI	Data Sains	2	13.33%	13	86.67%
	Internet of Things (IOT)	9	25.71%	26	74.29%
	IT Konsultan (GRC)	8	17.78%	37	82.22%
	Kecerdasan Buatan	7	28.00%	18	72.00%
	Keselamatan Siber	62	29.25%	150	70.75%
	Lain-lain	1	20.00%	4	80.00%
	Pelajar IPT	4	36.36%	7	63.64%
	Pembantu Teknikal	0	0.00%	1	100.00%
	Pengaturcaraan	1	100.00%	0	0.00%
	Pengkomputeran Awan	19	29.23%	46	70.77%
	Sistem Rangkaian	24	26.67%	66	73.33%

		Q10					
		Membantu		Sangat Membantu		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	10	66.67%	2	13.33%	3	20.00%
	Internet of Things (IOT)	13	37.14%	15	42.86%	7	20.00%
	IT Konsultan (GRC)	16	35.56%	21	46.67%	8	17.78%
	Kecerdasan Buatan	11	44.00%	10	40.00%	4	16.00%
	Keselamatan Siber	95	44.81%	84	39.62%	33	15.57%
	Lain-lain	1	20.00%	4	80.00%	0	0.00%
	Pelajar IPT	3	27.27%	6	54.55%	2	18.18%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	1	100.00%	0	0.00%	0	0.00%
	Pengkomputeran Awan	32	49.23%	24	36.92%	9	13.85%
	Sistem Rangkaian	44	48.89%	32	35.56%	14	15.56%

		Q11					
		Membantu		Sangat Membantu		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	12	80.00%	1	6.67%	2	13.33%
	Internet of Things (IOT)	16	45.71%	14	40.00%	5	14.29%
	IT Konsultan (GRC)	28	62.22%	11	24.44%	6	13.33%
	Kecerdasan Buatan	18	72.00%	2	8.00%	5	20.00%
	Keselamatan Siber	129	60.85%	45	21.23%	38	17.92%
	Lain-lain	2	40.00%	2	40.00%	1	20.00%
	Pelajar IPT	8	72.73%	1	9.09%	2	18.18%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	1	100.00%	0	0.00%	0	0.00%
	Pengkomputeran Awan	43	66.15%	14	21.54%	8	12.31%
	Sistem Rangkaian	59	65.56%	18	20.00%	13	14.44%

		Q12					
		Pantas		Sangat Pantas		Sederhana	
		Count	Row N %	Count	Row N %	Count	Row N %
PROFESI	Data Sains	12	80.00%	1	6.67%	2	13.33%
	Internet of Things (IOT)	31	88.57%	2	5.71%	2	5.71%
	IT Konsultan (GRC)	41	91.11%	3	6.67%	1	2.22%
	Kecerdasan Buatan	23	92.00%	1	4.00%	1	4.00%
	Keselamatan Siber	186	87.74%	5	2.36%	21	9.91%
	Lain-lain	5	100.00%	0	0.00%	0	0.00%
	Pelajar IPT	10	90.91%	1	9.09%	0	0.00%
	Pembantu Teknikal	0	0.00%	1	100.00%	0	0.00%
	Pengaturcaraan	1	100.00%	0	0.00%	0	0.00%
	Pengkomputeran Awan	53	81.54%	2	30.77%	10	15.38%
	Sistem Rangkaian	75	83.33%	7	7.78%	8	8.89%

Item 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Data Sains	15	3.0	3.0	3.0
	Internet of Things (IOT)	35	6.9	6.9	9.9
	IT Konsultan (GRC)	45	8.9	8.9	18.8
	Kecerdasan Buatan	25	5.0	5.0	23.8
	Keselamatan Siber	212	42.0	42.0	65.7
	Lain-lain	5	1.0	1.0	66.7
	Pelajar IPT	11	2.2	2.2	68.9
	Pembantu Teknikal	1	.2	.2	69.1
	Pengaturcaraan	1	.2	.2	69.3
	Pengkomputeran Awan	65	12.9	12.9	82.2
	Sistem Rangkaian	90	17.8	17.8	100.0
	Total	505	100.0	100.0	

Item 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Berkesan	321	63.6	63.6	63.6
	Sangat Berkesan	149	29.5	29.5	93.1
	Sederhana	35	6.9	6.9	100.0
	Total	505	100.0	100.0	

Item 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	111	22.0	22.0	22.0
	Sangat Membantu	394	78.0	78.0	100.0
	Total	505	100.0	100.0	

Item 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Memuaskan	411	81.4	81.4	81.4
	Sangat Memuaskan	69	13.7	13.7	95.0
	Sederhana	25	5.0	5.0	100.0
	Total	505	100.0	100.0	

Item 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	57	11.3	11.3	11.3
	Sangat Membantu	448	88.7	88.7	100.0
	Total	505	100.0	100.0	

Item 6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	76	15.0	15.0	15.0
	Sangat Membantu	429	85.0	85.0	100.0
	Total	505	100.0	100.0	

Item 7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agak Mempermudahkan	282	55.8	55.8	55.8
	Sangat Mempermudahkan	208	41.2	41.2	97.0
	Sederhana	15	3.0	3.0	100.0
	Total	505	100.0	100.0	

Item 8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agak Mempermudahkan	326	64.6	64.6	64.6
	Sangat Mempermudahkan	169	33.5	33.5	98.0
	Sederhana	10	2.0	2.0	100.0
	Total	505	100.0	100.0	

Item 9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agak Mempermudahkan	216	42.8	42.8	42.8
	Sangat Mempermudahkan	259	51.3	51.3	94.1
	Sederhana	30	5.9	5.9	100.0
	Total	505	100.0	100.0	

Item 10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	137	27.1	27.1	27.1
	Sangat Membantu	368	72.9	72.9	100.0
	Total	505	100.0	100.0	

Item 11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	226	44.8	44.8	44.8
	Sangat Membantu	199	39.4	39.4	84.2
	Sederhana	80	15.8	15.8	100.0
	Total	505	100.0	100.0	

Item 12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Membantu	316	62.6	62.6	62.6
	Sangat Membantu	109	21.6	21.6	84.2
	Sederhana	80	15.8	15.8	100.0
	Total	505	100.0	100.0	

Item 13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Pantas	437	86.5	86.5	86.5
	Sangat Pantas	23	4.6	4.6	91.1
	Sederhana	45	8.9	8.9	100.0
	Total	505	100.0	100.0	

RUMUSAN

Projek ini bertujuan untuk mengatasi ancaman siber yang semakin meningkat dengan mengembangkan strategi pengesanan dan pengenalpastian ancaman yang lebih inovatif dan berkesan. Kajian ini menggabungkan kerangka kerja MITRE ATT&CK, yang terkenal dengan taksonomi sistematiknya dalam maklumat ancaman siber (CTI), dengan model pembelajaran mendalam yang menggunakan rangkaian neural. Gabungan ini diharapkan dapat meningkatkan pemahaman dan pengesanan terhadap corak taktik, teknik, dan prosedur (TTP) yang berbilang, seperti yang digariskan dalam kerangka ATT&CK.

Dengan integrasi pembelajaran mendalam, sistem ini mampu mengadaptasi dan mengemas kini keupayaan pengesanan ancaman secara dinamik, sesuai dengan perkembangan taksonomi ATT&CK, memastikan maklumat kekal relevan dalam landskap ancaman yang sentiasa berubah. Di samping itu, kajian ini meneroka penggunaan arkitektur ancaman melalui STIX/TAXII dalam analisis data besar, selari dengan metodologi DevSecOps, untuk menyediakan strategi keselamatan siber yang lebih responsif dan adaptif. Pendekatan inovatif ini juga memperkenalkan efemeral graf visualisasi (EGV), yang menggunakan model peluruhan untuk menilai dan mengemas kini relevansi maklumat berdasarkan kejadian atau insiden tertentu, memberikan peningkatan kecekapan dalam proses analisis keselamatan (SA) dan mempercepatkan masa tindak balas.

Data kajian diperoleh secara masa nyata dari platform awan dan melalui proses sanitasi sebelum digunakan dalam Sistem Pengurusan Maklumat Keselamatan (SIEM). Proses ini termasuk normalisasi data, penggunaan Regex, dan pengaliran maklumat ancaman melalui saluran ETL. Dasar Sistem Pengesanan Pencerobohan (IDS) turut memainkan peranan penting dalam membantu pakar subjek (SME) merangka model pembelajaran mendalam (DLM) pada peringkat awal, dengan latihan berterusan untuk memastikan ketepatan dan keberkesanan. Penemuan awal menunjukkan bahawa efemeral graf visualisasi (EGV) menawarkan cara yang lebih intuitif dan efisien dalam memahami landskap ancaman yang kompleks berbanding kaedah tradisional, dengan menampilkan entiti data sebagai nod dan hubungan antaranya sebagai jalur dalam graf yang komprehensif. Kajian ini menandakan pendekatan yang bertransformasi dalam interpretasi dan maklum balas terhadap maklumat ancaman siber.

Kajian ini menekankan dua pencapaian objektif iaitu:

- Membangunkan sistem perwakilan data yang ringkas dalam bentuk graf nod yang diberi nama (EGV) tanpa memerlukan pengetahuan lanjutan untuk mengendalikan produk yang khusus

sepanjang proses penyiasatan

- Membina satu model pelajaran mendalam bagi tujuan pengkelasan serangan yang berterusan untuk mencapai orkestrasi alur kerja

dimana setiapa satunya mempunyai kebergantungan yang kompleks seperti yang diterangkan pada paparan **SEBELUMNYA.** Bagi objektif pertama, platform EGV dapat direalisasikan dengan pembentukan visual hubungan antara attribut. Walaubagaimanapun keperluan bagi menggunakan sepenuhnya fungsi yang berada pada **objektif 1** terletak di **objektif 2**. Dimana data yang besar diperlukan untuk melatih proses pengenalpastian ancaman supaya model dapat membantu dalam proses penyiasatan yang lebih teratur. Meskipun kekurangan jumlah data yang besar untuk mematangkan model pengesanan, objektif 2 turut dianggap berjaya kerana hasil orkestrasi kerja dapat dicapai dalam kajian ini dimana proses sanitasi daripada data mentah kepada attribut penting untuk pembelajaran berterusan dapat dihasilkan secara masa nyata. Sekaligus memudahkan algorithm pembelajaran mendalam membuat pengesanan dengan lebih tepat dibantu dengan kerangka MITRE dan CTI. Hasil kepada kedua-dua objektif ini dapat membuahkan suatu pemangkin untuk penjelajahan skop yang baharu, dimana dapat memberikan manfaat kepada industri penyedia perkhidmatan terutama sekali di dalam bidang keselamatan siber. Berdasarkan pencapaian objektif setakat ini, pelanggan (syarikat) amat berpuas hati dengan hasil yang diperoleh sepanjang kajian ini dijalankan. Hal ini kerana inovasi ini bukan sahaja mampu menarik minat daripada ahli bidang, malah juga professional dari industri keselamatan siber.

PENGHARGAAN

Dengan lafaz nama Allah yang maha pengasih lagi maha penyayang. Saya memanjatkan rasa syukur kepada Allah S.W.T atas nikmat kesihatan yang telah diberikan, yang mana membolehkan saya menyiapkan tesis kajian ini dengan jayanya. Penghargaan yang tulus saya ucapkan kepada penyelia projek saya, (Assoc. Prof. Dr.) Siti Norul Huda Sheikh Abdullah, atas tunjuk ajar, nasihat, teguran, dan dorongan yang telah diberikan. Bimbingan beliau amatlah berharga dalam membantu proses penyelesaian bagi kajian ini. Saya juga ingin menyampaikan penghargaan kepada semua pensyarah di Fakulti Teknologi dan Sains Maklumat (FTSM) diatas segala ilmu yang telah dicurahkan, yang mana telah membantu sebahagian besar daripada proses kajian ini. Tidak lupa juga ucapan terima kasih kepada rakan serta penyelia industri yang sudi meluangkan masa dan juga keringat bagi bersama-sama membantu dalam menjayakan kajian ini. Terutamanya kepada AceTeam Networks Sdn Bhd yang telah banyak memberikan input dan kerjasama di sepanjang proses kajian dijalankan. Akhir sekali, ucapan terima kasih yang tak terhingga juga kepada keluarga dan saudara seperjuangan yang tidak putus memberikan bantuan dan semangat di sepanjang proses penghasilan bagi tesis kajian projek akhir ini

RUJUKAN

A. A. Mustafar, N. F. Ainun Zainal, T. A. Mohd Tajul Ariffin, S. N. Huda Sheikh Abdullah, K. M. Daud and Y. T. Dun, "Cyber-attack Group Representation based on Adversary Artifacts with Machine Learning," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 01-06, doi: 10.1109/ICCR56254.2022.9995959.

A. Krizhevsky, I. Sutskever, and G. E. Hinton. 2012. "Imagenet classification with deep convolutional neural networks." *25th International Conference on Neural Information Processing Systems (NIPS).* Lake Tahoe, NV, USA: Neural Information Processing Systems Foundation. 1097 -1105.

Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, Alban Desmaison, Andreas Kopf, Edward Yang, Zachary DeVito, Martin Raison, Alykhan Tejani, Sasank Chilamkurth. 2019. "PyTorch: An Imperative Style, High-Performance Deep Learning Library." *Adv. Neural Inf. Process. Syst.*

Aechan Kim, Mohyun Park and Dong Hoon Lee. 2020. "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection." *IEEE* 70245 - 70253.

Aloqaily, Moayad, Salil Kanhere, Paolo Bellavista, dan Michele Nogueira. 2022. *Aloqaily, Moayad, Salil Kanhere, Paolo Bellavista, dan Michele Nogueira.* March 18. https://link.springer.com/article/10.1007/s10922-022-09659-3.

Aminanto, K. Kim and M. E. 2017. "Deep learning in intrusion detection perspective: Overview and further challenge." *2017 International Workshop on Big Data and Information Security (IWBIS)* 5-10.

Anna Georgiadou, * Spiros Mouzakitis, and Dimitris Askounis. 2021. *National Center for Biotechnology Information (NCBI).* May 9. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8125987/#:~:text=2,knowledge%20base%20of%20cy ber.

B. Mukherjee, L. T. Heberlein, and K. N. Levitt. 1994. "Network intrusion detection." *EEE Network* 26 - 41.

Bader Al-Sada, Alireza Sadighian and Gabriele Oligeri. 2023. "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database." *IEEE* 1217 - 1234.

Beeceptor. n.d. *Web Data Serialization - JSON, XML, YAML & More Explained.* Accessed January 6, 2023. https://beeceptor.com/docs/concepts/data-exchange-formats/.

Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas. 2018. "Design and Philosophy." *MITRE ATT&CK.*

Bowers, Michael Agun and Shawn. 2011. "Approaches for Implementing Persistent Queues within Data- Intensive Scientific Workflows." *Services (SERVICES), 2011 IEEE World Congress* . Research Gate.

Calzon, Bernardita. 2023. *Understanding Data Drill Down And Drill Through Analysis And Their Role In Efficient Reporting.* March 10. Accessed January 6, 2024. https://www.datapine.com/blog/drill-down-drill-through-reports/.

Chaolun Xia, Xiaohong Jiang, Sen LIu, Zhaobo Luo, and Zhang Yu. 2010. "Dynamic Item-Based Recommendation Algorithm." *ResearchGate* 242–247.

CloudTamers. 2023. *8 Ways Data Visualisation Dashboards Will Put You in Charge of Your Data.* October 16. Accessed January 19, 2024. https://www.linkedin.com/pulse/8-ways-data-visualisation-dashboards- put-you-charge-your-xjgxe/.

E. Dasseni, V. S. Verykios, A. K. Elmagarmid and E. Bertino. 2001. "Hiding Association Rules by Using Confidence and Support." *SpringerLink* 369-383.

Goldberg, Joe. 2022. *Orchestrate and Automate to Make DataOps Successful.* October 3. Accessed January 1, 2024. https://www.bmc.com/blogs/dataops-orchestration/.

Gourav Jain, Tripti Mahara, Subhash Chander Sharma, Saurabh Agarwal and Hyungsung kim. 2022. "TD-DNN: A Time Decay-Based Deep Neural Network for Recommendation System." *TD-DNN: A Time Decay-Based Deep Neural Network for Recommendation System* 2-22.

Guven, A. L. Buczak and E. 2016. "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Commun. Surv. Tutor.* 1153 - 1176.

Houyi, Pan. 2023. *The main cyber risk that defenders worry about is "misconfiguration of security equipment".* April 21. Accessed January 18, 2024. https://cybersecurenews.com.tw/expert-talk-025/.

Innes, Matthew. 2023. *SIEM Demystified: How This Technology Safeguards Your Digital World.* September 12. Accessed January 14, 2024. https://securitygladiators.com/security/software/siem/.

Juha Karhunen, Tapani Raiko, and KyungHyun Cho 2. 2015. "Unsupervised deep learning: A short review." *Advances in Independent Component Analysis and Learning Machines* 125-142.

Kirvan, Paul. 2023. *What is ISACA?* August 14. https://www.techtarget.com/searchcio/definition/ISACA. Kobialka, Dan. 2022. *Sophos 2023 Threat Report: Cybercrime-as-a-Service on the Rise.* November 21. Accessed December 14, 2023. https://www.msspalert.com/news/sophos-2023-threat-report-cybercrime-as-a-service-on-the-rise.

Kuner, Christopher, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, dan Christopher Millard. 2017. "International Data Privacy Law." *The rise of cybersecurity and its impact on data protection* 73–75.

Lakshmi Narayanan Kaliyaperumal, CISA, CISM, EnCE, GNFA. 2021. *The Evolution of Security Operations and Strategies for Building an Effective SOC.* October 26. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc.

M. Atallah, E. Bertino, A. Elmagarmid, M. Ibrahim and V. Verykios. 1999. "Disclosure Limitation of Sensitive Rules." *IEEE* 45-52.

Mahmood, A Shrestha and A. 2019. "Review of deep learning algorithms and architectures." *IEEE* 53040– 53065.

McMillan, Rob. 2013. *Definition: Threat Intelligence.* May 16. Accessed January 18, 2024.

N. Naik, Paul Jenkins, P. Grace, Jingping Song. 2022. *Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model.* October 24. https://www.semanticscholar.org/paper/Comparing-Attack-Models-for-IT-Systems%3A-Lockheed-Naik-Jenkins/520a433a4ecb2ace75ded2a1243615bef74ed985.

Nickles, Katie. 2019. *Getting Started with ATT&CK: Threat Intelligence.* June 10. Accessed December 14, 2023. https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f.

Ninja, Team. 2023. *IT Automation Scripts: Definition and Overview.* November 15. Accessed January 2, 2024. https://www.ninjaone.com/blog/it-automation-scripts-definition-and-overview/.

OASIS. 2023. *Introduction to STIX.* September 23. Accessed January 6, 2024. https://oasis-open.github.io/cti-documentation/.

P. Chen, L. Desmet and C. Huygens,. 2014. "A study on advanced persistent threats." *Proc. IFIP Int. Conf. Commun. Multimedia Secur.* 63-72.

P. R. Vishnu, P. Vinod & Suleiman Y. Yerima. 2021. *A Deep Learning Approach for Classifying Vulnerability Descriptions Using Self Attention Based Neural Network.* October 8. https://link.springer.com/article/10.1007/s10922-021-09624-6.

Reed, Jonathan. 2022. *Hiring and retention in the cybersecurity workforce remain difficult.* October 5. https://securityintelligence.com/news/cybersecurity-hiring-retention-2022/.

Sahai, Mukul Kumar and Anupam. 2016. *Turn the NIST Cybersecurity Framework into Reality: 5 Steps.* September 20. Accessed January 18, 2024. https://www.darkreading.com/cybersecurity-analytics/turn-the-nist-cybersecurity-framework-into-reality-5-steps.

Saini, Rahul. 2023. *Analytics Dashboard : Unlocking Data-Driven Decision Making.* November 1. Accessed January 19, 2024. https://growthnatives.com/blogs/analytics/analytics-dashboard-unlocking-data-driven-decision-making/.

Sharma, B. Chandra and R. K. 2016. "Deep learning with adaptive learning rate using laplacian score." *Exp. Syst. Appl* 1-7.

Skopik, Florian, dan Timea Pahi. 2020. *Under false flag: using technical artifacts for cyber attack attribution.* March 20. https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4.

Sophos. 2023. *The State of Cybersecurity 2023: The Business Impact of Adversaries.* April. Accessed December 14, 2023. https://assets.sophos.com/X24WTUEQ/at/f8t5qgvm44h5s39br4pkcjt/sophos-the- state-of-cybersecurity-2023-wp.pdf.

Splunk. 2023. August 25. Accessed January 19, 2024. https://docs.splunk.com/Documentation/Splunk/9.1.2/Data/Usepersistentqueues.

—. 2018. *Clearer Insights and Investigations: Splunk Enterprise Security 5.1.* May 14. Accessed January 20, 2024. https://www.splunk.com/en_us/blog/security/clearer-insights-and-investigations-splunk-enterprise-security-5-1.html?301=/blog/2018/05/14/clearer-insights-and-investigations-splunk- enterprise-

security-5-1.html&utm_source=linkedin&utm_medium=organicsocial&li.

—. 2023. *Use persistent queues to help prevent data loss.* August 25. Accessed January 19, 2024. https://docs.splunk.com/Documentation/Splunk/9.1.2/Data/Usepersistentqueues.

Staron, Miroslaw. 2015. "Dashboard development guide How to build sustainable and useful dashboards to support software development and maintenance." Research Report, Gothenburg.

Trivedi, Coral. 2023. *Navigating Data Lake Challenges: Governance, Security, and Automation.* August 10. Accessed January 6, 2024. https://tdwi.org/articles/2023/08/10/arch-all-navigating-data-lake-governance-security-and-automation.aspx.

W. Fu, X. Xin, P. Guo and Z. Zhou. 2016. "A practical intrusion detection system for internet of vehicles." *China Communications* 263-275.

n.d. *What is the mitre att&ck framework.* Accessed January 14, 2024. https://www.sentinelone.com/cybersecurity-101/mitre-attack-framework/#:~:text=Introduction,objective%20%E2%80%93%20think%20data.

Y. LeCun, Y. Bengio, and G. Hinton. 2015. "Deep learning." *Nature* 436–444.

Yadav, Sanjeev. 2023. *Importance of Data Sanitization.* December 26. Accessed January 19, 2024. https://www.bitraser.com/article/importance-of-data-sanitization.php.

Yann LeCun, Yoshua Bengio and Geoffrey Hinton. 2015. "Deep learning." *Nature* 436–444.

YC Chen, L Hui and T Thaipisutikul. 2021. "A collaborative filtering recommendation system with dynamic time decay." *IEEE* 244–262.

Yu, Li Deng and Dong. 2013. "Deep Learning: Methods and Applications." *Found. Trends Signal Process* 197–387.

Yu, Sen. 2016. *How to Make Your Persistent Queues Run Faster Safely.* May 4. Accessed January 21, 2024. https://eng.wealthfront.com/2016/05/04/how-to-make-your-persistent-queues-run-faster-safely/.

Zaiane, S.R.M. Oliveira and O.R. 2002. "Algorithms for balancing privacy and knowledge discovery in association rule mining." *IEEE* 43-54.

Ahmad Asyraf Bin Mustafar (A185868)

Assoc. Prof. Dr. Siti Norul Huda Sheikh Abdullah

Fakulti Teknologi & Sains Maklumat

Universiti Kebangsaan Malaysia